离散数学

左孝凌　李为鑑　刘永才　编著

LISAN SHUXUE

上海科学技术文献出版社

目　录

第一篇 数理逻辑

逻辑学是一门研究思维形式及思维规律的科学。逻辑规律就是客观事物在人的主观意识中的反映。

逻辑学分为辩证逻辑与形式逻辑两种，前者是以辩证法认识论的世界观为基础的逻辑学，而后者主要是对思维的形式结构和规律进行研究的类似于语法的一门工具性学科。思维的形式结构包括了概念，判断和推理之间的结构和联系，其中概念是思维的基本单位，通过概念对事物是否具有某种属性进行肯定或否定的回答，这就是判断；由一个或几个判断推出另一判断的思维形式，就是推理。研究推理有很多方法，用数学方法来研究推理的规律称为数理逻辑。这里所指的数学方法，就是引进一套符号体系的方法，所以数理逻辑又称作符号逻辑，它是从量的侧面来研究思维规律的。

现代数理逻辑可分为证明论、模型论、递归函数论、公理化集合论等，这里介绍的是数理逻辑最基本的内容：命题逻辑和谓词逻辑。

第一章　命题逻辑

1-1　命题及其表示法

在数理逻辑中，为了表达概念，陈述理论和规则，常常需要应用语言进行描述，但是日常使用的自然语言，往往叙述时不够确切，也易产生二义性，因此就需要引入一种目标语言，这种目标语言和一些公式符号，就形成了数理逻辑的形式符号体系。所谓目标语言就是表达判断的一些语言的汇集，而判断就是对事物有肯定或否定的一种思维形式，因此能表达判断的语言是陈述句，它称作命题。一个命题，总是具有一个“值”，称为真值。真值只有“真”和“假”两种，记作 True（真）和 False（假），分别用符号 $\boldsymbol{T}$ 和 $\boldsymbol{F}$ 表示。只有具有确定真值的陈述句才是命题，一切没有判断内容的句子，无所谓是非的句子，如感叹句，疑问句，祈使句等都不能作为命题。命题有两种类型：第一种类型是不能分解为更简单的陈述语句，称作原子命题；第二种类型是由联结词，标点符号和原子命题复合构成的命题，称作复合命题。所有这些命题，都应具有确定的真值。下面给出实例，说明命题的概念。

(1) 中国人民是伟大的。

(2) 雪是黑的。

(3) $1+101=110$

(4) 别的星球上有生物。

(5) 全体立正！

(6) 明天是否开大会？

(7) 天气多好啊！

(8) 我正在说谎。

(9) 我学英语，或者我学日语。

(10) 如果天气好，那么我去散步。

在上面这些例子中，(1)、(2)、(4)、(9)、(10)是命题。其中(9)、(10)是复合命题，(4)在目前可能无法决定真值，但从事物的本质而论，它本身是有真假可言的，所以我们承认这也是一个命题。(5)、(6)、(7)都不是命题。(8)是悖论。(3)在二进制中为真，在十进制中为假，故需根据上下文才能确定真值。

在数理逻辑中，我们将使用大写字母 $A, B, \cdots, P, Q, \cdots$ 或用带下标的大写字母或用数字，如 A_i, [12] 等表示命题，例如

P: 今天下雨。

P 可表示"今天下雨"这个命题的名。亦可用数字表示命题，例如

[12]: 今天下雨。

表示命题的符号称为命题标识符，P 和 [12] 就是标识符。

一个命题标识符如表示确定的命题，就称为命题常量，如果命题标识符只表示任意命题的位置标志，就称为命题变元。因为命题变元可以表示任意命题，所以它不能确定真值，故命题变元不是命题。当命题变元 P 用一个特定命题取代时，P 才能确定真值，这时也称对 P 进行指派。当命题变元表示原子命题时，该变元称为原子变元。

1-2 联结词

在自然语言中，常常使用"或"，"与"，"但是"等一些联结词，对于这种联结词的使用，一般没有很严格的定义，因此有时显得不很确切。在数理逻辑中，复合命题是由原子命题与逻辑联结词组合而成，联结词是复合命题中的重要组成部分，为了便于书写和进行推演，必须对联结词作出明确规定并符号化。下面介绍各个联结词。

(1) 否定

定义 1-2.1 设 P 为一命题，P 的否定是一个新的命题，记作 $\neg P$。若 P 为 T, $\neg P$ 为 F；若 P 为 F, $\neg P$ 为 T。联结词

1111237

“$\neg$”表示命题的否定。否定联结词有时亦可记作“—”。

命题 P 与其否定 $\neg P$ 的关系如表 1-2.1 所示。

表 1-2.1

P	$\neg P$
T	**F**
F	**T**

例　　　P：上海是一个大城市。

　　　$\neg P$：上海并不是一个大城市。

或　　　$\neg P$：上海是一个不大的城市。

这两个命题用同一符号 $\neg P$ 表示，因为在汉语中这两个命题具有相同的意义。

“否定”的意义仅是修改了命题的内容，我们仍把它看作为联结词，它是一个一元运算。

(2) 合取

定义 1-2.2　两个命题 P 和 Q 的合取是一个复合命题，记作 $P\wedge Q$。当且仅当 P、Q 同时为 **T** 时，$P\wedge Q$ 为 **T**，在其他情况下，$P\wedge Q$ 的真值都是 **F**。

联结词“$\wedge$”的定义如表 1-2.2 所示。

表 1-2.2

P	Q	$P\wedge Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

例如　　　P：今天下雨。

　　　Q：明天下雨。

上述命题的合取为

$P\wedge Q$：今天下雨而且明天下雨。

$P\wedge Q$：今天与明天都下雨。

$P\wedge Q$：这两天都下雨。

显然只有当“今天下雨”与“明天下雨”都是真时，“这两天都下雨”才是真的。

合取的概念与自然语言中的“与”意义相似，但并不完全相同。例如

P：我们去看电影。

Q：房间里有十张桌子。

上述命题的合取为

$P\wedge Q$：我们去看电影与房间里有十张桌子。

在自然语言中，上述命题是没有意义的，因为 P 与 Q 没有内在联系，但作为数理逻辑中 P 和 Q 的合取 $P\wedge Q$ 来说，它仍可成为一个新的命题，只要按照定义，在 P、Q 分别取真值后，$P\wedge Q$ 的真值也必确定。

命题联结词“合取”甚至可以将两个互为否定的命题联结在一起。这时，其真值永为 $\boldsymbol{F}$。

命题联结词“合取”也可以将若干个命题联结在一起。

“合取”是一个二元运算。

(3) 析取

定义 1-2.3 两个命题 P 和 Q 的析取是一个复合命题，记作 $P\vee Q$。当且仅当 P、Q 同时为 $\boldsymbol{F}$ 时，$P\vee Q$ 的真值为 $\boldsymbol{F}$，否则 $P\vee Q$ 的真值为 $\boldsymbol{T}$。

联结词“$\vee$”的定义如表 1-2.3 所示。

表 1-2.3

P	Q	$P\vee Q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

从析取的定义可以看到，联结词 $\vee$ 与汉语中的“或”的意义也不全相同，因为汉语中的“或”，可表示“排斥或”，也可表示“可兼或”。

例 1　今天晚上我在家看电视或去剧场看戏。

例 2　他可能是 100 米或 400 米赛跑的冠军。

在例 1 中的“或”是“排斥或”，例 2 中的“或”是“可兼或”，而析取指的是“可兼或”。还有一些汉语中的“或”字，实际不是命题联结词。

例 3　他昨天做了二十或三十道习题。

这个例子中的“或”字，只表示了习题的近似数目，不能用联结词“析取”表达，例 3 是个原子命题。

(4) 条件

定义 1-2.4　给定两个命题 P 和 Q，其条件命题是一个复合命题，记作 $P\rightarrow Q$，读作“如果 P，那末 Q”或“若 P 则 Q”。当且仅当 P 的真值为 $\boldsymbol{T}$，Q 的真值为 $\boldsymbol{F}$ 时，$P\rightarrow Q$ 的真值为 $\boldsymbol{F}$，否则 $P\rightarrow Q$ 的真值为 $\boldsymbol{T}$。我们称 P 为前件，Q 为后件。

联结词“$\rightarrow$”的定义如表 1-2.4 所示。

表 1-2.4

P	Q	$P\rightarrow Q$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{T}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{T}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{T}$

例 1　如果某动物为哺乳动物，则它必胎生。

例 2　如果我得到这本小说，那末我今夜就读完它。

例 3　如果雪是黑的，那末太阳从西方出。

上述三个例子都可用条件命题 $P\rightarrow Q$ 表达。

在自然语言中，“如果…”与“那末…”之间常常是有因果联系

的，否则就没有意义，但对条件命题 $P \rightarrow Q$ 来说，只要 P、Q 能够分别确定真值，$P \rightarrow Q$ 即成为命题。此外，自然语言中对"如果…、则…"这样的语句，当前提为假时，结论不管真假，这个语句的意义，往往无法判断。而在条件命题中，规定为"善意的推定"，即前提为 $\boldsymbol{F}$ 时，条件命题的真值都取为 $\boldsymbol{T}$。

在数学上和有些逻辑学的书籍中，"若 P 则 Q" 亦可叫作 P 蕴含 Q，而本书在条件命题中将避免使用"蕴含"一词，因为在以后将另外定义"蕴含"这个概念。

命题联结词"$\rightarrow$"亦可记作"$\supset$"。条件联结词亦是二元运算。

(5) 双条件

定义 1-2.5 给定两个命题 P 和 Q，其复合命题 $P \rightleftarrows Q$ 称作双条件命题，读作"P 当且仅当 Q"，当 P 和 Q 的真值相同时，$P \rightleftarrows Q$ 的真值为 $\boldsymbol{T}$，否则 $P \rightleftarrows Q$ 的真值为 $\boldsymbol{F}$。

联结词"$\rightleftarrows$"的定义可如表 1-2.5 所示。

表 1-2.5

P	Q	$P \rightleftarrows Q$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{T}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{T}$

例 1 两个三角形全等，当且仅当它们的三组对应边相等。

例 2 燕子飞回南方，春天来了。

例 3 $2+2=4$ 当且仅当雪是白的。

上面三个例子都可用双条件命题 $P \rightleftarrows Q$ 来表示。与前面的联结词一样，双条件命题也可以不顾其因果联系，而只根据联结词定义确定真值。双条件联结词亦可记作"$\leftrightarrow$"或"iff"。它亦是二元运算。

1-1, 1-2 习题

(1) 指出下列语句哪些是命题，哪些不是命题，如果是命题，指出它的真值。

a) 离散数学是计算机科学系的一门必修课。

b) 计算机有空吗？

c) 明天我去看电影。

d) 请勿随地吐痰！

e) 不存在最大质数。

f) 如果我掌握了英语、法语，那么学习其他欧洲语言就容易得多。

g) $9+5\leqslant 12$

h) $x=3$

i) 我们要努力学习。

(2) 举例说明原子命题和复合命题。

(3) 设 P 表示命题“天下雪”

Q 表示命题“我将去镇上”

R 表示命题“我有时间”

以符号形式写出下列命题。

a) 如果天不下雪和我有时间，那么我将去镇上。

b) 我将去镇上，仅当我有时间时。

c) 天不下雪。

d) 天下雪，那么我不去镇上。

(4) 用汉语写出一句子，对应下列每一个命题。

a) $Q \rightleftarrows (R \wedge \neg P)$

b) $R \wedge Q$

c) $(Q \rightarrow R) \wedge (R \rightarrow Q)$

(5) 将下列命题符号化。

a) 王强身体很好，成绩也很好。

b) 小李一边看书，一边听音乐。

c) 气候很好或很热。

d) 如果 a 和 b 是偶数，则 $a+b$ 是偶数。

e) 四边形 $ABCD$ 是平行四边形，当且仅当它的对边平行。

f) 停机的原因在于语法错误或程序错误。

(6) 将下列复合命题分成若干原子命题。

a) 天气炎热且正在下雨。

b) 天气炎热但湿度较低。

c) 天正在下雨或湿度很高。

d) 刘英与李进上山。

e) 老王或小李是革新者。

f) 如果你不看电影，那么我也不看电影。

g) 我既不看电视也不外出，我在睡觉。

h) 控制台打字机既可作输入设备，又可作输出设备。

1-3 命题公式与翻译

前面已经提到，不包含任何联结词的命题叫做原子命题，至少包含一个联结词的命题称作复合命题。

设 P 和 Q 是任意两个命题，则 $\neg P$, $P\vee Q$, $(P\vee Q)\vee(P\rightarrow Q)$, $P\rightleftarrows(Q\vee\neg P)$ 等都是复合命题。

若 P 和 Q 是命题变元，则上述各式均称作命题公式。P 和 Q 称作命题公式的分量。

必须注意：命题公式是没有真假值的，仅当在一个公式中命题变元用确定的命题代入时，才得到一个命题。这个命题的真值，依赖于代换变元的那些命题的真值。此外，并不是由命题变元，联结词和一些括号组成的字符串都能成为命题公式。

定义 1-3.1 命题演算的合式公式(wff)，规定为：

(1) 单个命题变元本身是一个合式公式。

(2) 如果 A 是合式公式，那么 $\neg A$ 是合式公式。

(3) 如果 A 和 B 是合式公式，那么 $(A\wedge B)$, $(A\vee B)$, $(A\rightarrow B)$ 和 $(A\rightleftarrows B)$ 都是合式公式。

(4) 当且仅当能够有限次地应用(1)、(2)、(3)所得到的包含命题变元，联结词和括号的符号串是合式公式。

这个合式公式的定义，是以递归形式给出的，其中(1)称为基础，(2)(3)称为归纳，(4)称为界限。

按照定义，下列公式都是合式公式：

$$\neg(P\wedge Q),\ \neg(P\to Q),\ (P\to(P\vee\neg Q)),$$
$$(((P\to Q)\wedge(Q\to R))\rightleftarrows(S\rightleftarrows T))$$

而

$$(P\to Q)\to(\wedge Q),\ (P\to Q,\ (P\wedge Q)\to Q)$$

等都不是合式公式。

为了减少使用圆括号的数量，约定最外层圆括号可以省略。

如果我们规定了联结词运算的优先次序为：$\neg$、$\wedge$、$\vee$、$\to$、$\rightleftarrows$，则 $P\wedge Q\to R$ 也是合式公式。

有了联结词的合式公式概念，我们可以把自然语言中的有些语句，翻译成数理逻辑中的符号形式。

例题1 试以符号形式写出命题：我们要做到身体好、学习好、工作好，为祖国四化建设而奋斗。

解 找出各原子命题，并用命题符号表示：

A：我们要做到身体好。

B：我们要做到学习好。

C：我们要做到工作好。

P：我们要为祖国四化建设而奋斗。

故命题可形式化为：$(A\wedge B\wedge C)\rightleftarrows P$

例题2 上海到北京的14次列车是下午五点半或六点开。

解 P：上海到北京的14次列车是下午五点半开。

Q：上海到北京的14次列车是下午六点开。

在本例中，汉语的"或"是不可兼或，而逻辑联结词 $\vee$ 是"可兼或"，因此不能直接对两命题析取。构造表如表1-3.1所示。

表 1-3.1

P	Q	原命题	$P\rightleftarrows Q$	$\neg(P\rightleftarrows Q)$
T	**T**	**F**	**T**	**F**
T	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**T**
F	**F**	**F**	**T**	**F**

从表中可看出原命题不能用前述五个联结词单独写出，但是如用命题和联结词组合，可以把本命题表达为：$\neg(P\rightleftarrows Q)$。

例题3 他既聪明又用功。

解 若设

P: 他聪明。 Q: 他用功。

在自然语言中这个"既……又……"显然与"且"的意义一样，故本例可记为:

$$P \wedge Q$$

例题4 他虽聪明但不用功。

解 这里"虽……但……"这个词不能用前述联结词表达，但其实际意义是：他聪明且不用功。若设

P: 他聪明。 Q: 他用功。

本例可表示为:

$$P \wedge \neg Q$$

例题5 除非你努力，否则你将失败。

解 这个命题的意义，亦可理解为：如果你不努力则你将失败。若设

P: 你努力。 Q: 你失败。

本例可表示为:

$$\neg P \rightarrow Q$$

例题6 张三或李四都可以做这件事。

解 这个命题的意义是：张三可以做这件事，并且李四也可以做这件事。若设

P: 张三可以做这事。 Q: 李四可以做这事。

本例可表示为:

$$P \wedge Q$$

从上面的例子中可以看到，自然语言中的一些联结词，如："与""且""或""除非…则…"等等都各有其具体含义，因此需分别不同情况翻译成适当的逻辑联结词。为了便于正确表达命题间的相互关系，有时也常常采用列出"真值表"的方法，进一步分析各原命题，以此寻找逻辑联结词，使原来的命题能够正确地用形式符号予以表达。

1-3 习题

(1) 判别下列公式哪些是合式公式，哪些不是合式公式。

a) $(Q \rightarrow R \wedge S)$

b) $(P \rightleftarrows (R \rightarrow S))$

c) $((\neg P \rightarrow Q) \rightarrow (Q \rightarrow P)))$

d) $(RS \to T)$

e) $((P \to (Q \to R)) \to ((P \to Q) \to (P \to R)))$

(2) 根据合式公式的定义，说明下列公式是合式公式。

a) $(A \to (A \vee B))$

b) $((\neg A \wedge B) \wedge A)$

c) $((\neg A \to B) \to (B \to A))$

d) $((A \to B) \vee (B \to A))$

(3) 对下列各式用指定的公式进行代换。

a) $(((A \to B) \to B) \to A)$，用 $(A \to C)$ 代换 A，用 $((B \wedge C) \to A)$ 代换 B。

b) $((A \to B) \vee (B \to A))$，用 B 代换 A。

(4) 下列几个式子中有哪几个是别的式子经过代换得到的。

a) $(P \to (Q \to P))$

b) $((((P \to Q) \wedge (R \to S)) \wedge (P \vee R)) \to (Q \vee S))$

c) $(Q \to ((P \to P) \to Q))$

d) $(P \to ((P \to (Q \to P)) \to P))$

e) $(((R \to S) \wedge (Q \to P)) \wedge (R \vee Q)) \to (S \vee P))$

(5) 试把原子命题表示为 P、Q、R 等，然后用符号译出下列各句子。

a) 或者你没有给我写信，或者它在途中丢失了。

b) 如果张三和李四都不去，他就去。

c) 我们不能既划船又跑步。

d) 如果你来了，那末他唱不唱歌将看你是否伴奏而定。

(6) 一个人起初说，“占据空间的、有质量的而且不断变化的叫做物质”；后来他改说，“占据空间的有质量的叫做物质，而物质是不断变化的。”问他前后主张的差异在什么地方，试以命题形式进行分析。

(7) 用符号形式写出下列命题。

a) 假如上午不下雨，我去看电影，否则就在家里读书或看报。

b) 我今天进城，除非下雨。

c) 仅当你走我将留下。

1-4 真值表与等价公式

定义 1-4.1 在命题公式中，对于分量指派真值的各种可能组合，就确定了这个命题公式的各种真值情况，把它汇列成表，就

是命题公式的真值表。

现举例说明如下：

例题 1 构造$\neg P \vee Q$的真值表。

解

表 1-4.1

P	Q	$\neg P$	$\neg P \vee Q$
T	**T**	**F**	**T**
T	**F**	**F**	**F**
F	**T**	**T**	**T**
F	**F**	**T**	**T**

例题 2 给出$(P \wedge Q) \wedge \neg P$的真值表。

解

表 1-4.2

P	Q	$P \wedge Q$	$\neg P$	$(P \wedge Q) \wedge \neg P$
T	**T**	**T**	**F**	**F**
T	**F**	**F**	**F**	**F**
F	**T**	**F**	**T**	**F**
F	**F**	**F**	**T**	**F**

例题 3 给出$(P \wedge Q) \vee (\neg P \wedge \neg Q)$的真值表。

解

表 1-4.3

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg P \wedge \neg Q$	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$
T	**T**	**F**	**F**	**T**	**F**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**T**	**F**	**F**	**F**	**F**
F	**F**	**T**	**T**	**F**	**T**	**T**

例题 4 给出$\neg(P \wedge Q) \rightleftarrows (\neg P \vee \neg Q)$的真值表。

解

表 1-4.4

P	Q	$P\wedge Q$	$\neg(P\wedge Q)$	$\neg P$	$\neg Q$	$\neg P\vee\neg Q$	$\neg(P\wedge Q)\rightleftarrows(\neg P\vee\neg Q)$
T	**T**	**T**	**F**	**F**	**F**	**F**	**T**
T	**F**	**F**	**T**	**F**	**T**	**T**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**	**T**

由表1-4.4(表1-4.2)可以看出，有一类公式不论命题变元作何种指派，其真值永为真(假)，我们把这类公式记为 **T**(**F**)。

在真值表中，命题公式真值的取值数目，决定于分量的个数。例如，由2个命题变元组成的命题公式共有四种可能的真值，由3个命题变元组成的命题公式共有八种真值。一般说来，n 个命题变元组成的命题公式共有 2^n 种真值情况。

从真值表中可以看到，有些命题公式在分量的不同指派下，其对应的真值与另一命题公式完全相同，如 $\neg P\vee Q$ 与 $P\rightarrow Q$ 的对应真值相同，如表1-4.5所示。

表 1-4.5

P	Q	$\neg P\vee Q$	$P\rightarrow Q$
T	**T**	**T**	**T**
T	**F**	**F**	**F**
F	**T**	**T**	**T**
F	**F**	**T**	**T**

同理 $(P\wedge Q)\vee(\neg P\wedge\neg Q)$ 与 $P\rightleftarrows Q$ 对应的真值相同，如表1-4.6所示。

表 1-4.6

P	Q	$P\rightleftarrows Q$	$(P\wedge Q)\vee(\neg P\wedge\neg Q)$
T	**T**	**T**	**T**
T	**F**	**F**	**F**
F	**T**	**F**	**F**
F	**F**	**T**	**T**

定义 1-4.2 给定两个命题公式 A 和 B，设 $P_1, P_2, \cdots, P_n$ 为所有出现于 A 和 B 中的原子变元，若给 $P_1, P_2, \cdots, P_n$ 任一组真值指派，A 和 B 的真值都相同，则称 A 和 B 是等价的或逻辑相等。记作 $A \Leftrightarrow B$。

例题 5 证明 $P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$

证明 列出真值表

表 1-4.7

P	Q	$P \to Q$	$Q \to P$	$P \rightleftarrows Q$	$(P \to Q) \wedge (Q \to P)$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**
F	**T**	**T**	**F**	**F**	**F**
F	**F**	**T**	**T**	**T**	**T**

由表 1-4.7 可知 $P \rightleftarrows Q$ 与 $(P \to Q) \wedge (Q \to P)$ 真值相同，命题得证。

表 1-4.8 列出的命题定律，都可以用真值表予以验证。

表 1-4.8

对合律	$\neg\neg P \Leftrightarrow P$	1
幂等律	$P \vee P \Leftrightarrow P$, $P \wedge P \Leftrightarrow P$	2
结合律	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	3
交换律	$P \vee Q \Leftrightarrow Q \vee P$ $P \wedge Q \Leftrightarrow Q \wedge P$	4
分配律	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	5
吸收律	$P \vee (P \wedge Q) \Leftrightarrow P$ $P \wedge (P \vee Q) \Leftrightarrow P$	6
德·摩根律	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	7
同一律	$P \vee \mathbf{F} \Leftrightarrow P$, $P \wedge \mathbf{T} \Leftrightarrow P$	8
零律	$P \vee \mathbf{T} \Leftrightarrow \mathbf{T}$, $P \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	9
否定律	$P \vee \neg P \Leftrightarrow \mathbf{T}$, $P \wedge \neg P \Leftrightarrow \mathbf{F}$	10

例题6 验证吸收律 $P \vee (P \wedge Q) \Leftrightarrow P$

$P \wedge (P \vee Q) \Leftrightarrow P$

证明 列出真值表

表 1-4.9

P	Q	$(P \wedge Q)$	$P \vee (P \wedge Q)$	$(P \vee Q)$	$P \wedge (P \vee Q)$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**T**	**T**
F	**T**	**F**	**F**	**T**	**F**
F	**F**	**F**	**F**	**F**	**F**

由表1-4.9可知吸收律成立。

在一个命题公式中，如果用公式置换命题的某个部分，一般地将会产生某种新的公式，例如 $Q \rightarrow (P \vee (P \wedge Q))$ 中以 $(\neg P \rightarrow Q)$ 取代 $(P \wedge Q)$，则 $Q \rightarrow (P \vee (\neg P \rightarrow Q))$ 就与原式不同。为了保证取代后的公式与原始公式是等价的，故需对置换作出一些规定。

定义1-4.3 如果 X 是合式公式 A 的一部分，且 X 本身也是一个合式公式，则称 X 为公式 A 的子公式。

定理1-4.1 设 X 是合式公式 A 的子公式，若 $X \Leftrightarrow Y$，如果将 A 中的 X 用 Y 来置换，所得到公式 B 与公式 A 等价，即 $A \Leftrightarrow B$。

证明 因为在相应变元的任一种指派情况下，X 与 Y 的真值相同，故以 Y 取代 X 后，公式 B 与公式 A 在相应的指派情况下，其真值亦必相同，故 $A \Leftrightarrow B$。 □

满足定理1-4.1条件的置换称为等价置换(等价代换)。

例题7 证明 $Q \rightarrow (P \vee (P \wedge Q)) \Leftrightarrow Q \rightarrow P$

证明 设 A: $Q \rightarrow (P \vee (P \wedge Q))$

因为 $P \vee (P \wedge Q) \Leftrightarrow P$

故 B: $Q \rightarrow P$，即 $A \Leftrightarrow B$

对 $A \Leftrightarrow B$ 亦可用表1-4.10予以验证：

表 1-4.10

P	Q	$P\wedge Q$	$P\vee(P\wedge Q)$	$Q\rightarrow(P\vee(P\wedge Q))$	$Q\rightarrow P$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**T**	**T**
F	**T**	**F**	**F**	**F**	**F**
F	**F**	**F**	**F**	**T**	**T**

我们有了最基本的命题公式的等价关系，再利用定理1-4.1，就可以推证一些更为复杂的命题等价公式。现举例说明如下：

例题 8 证明 $(P\wedge Q)\vee(P\wedge\neg Q)\Leftrightarrow P$

证明 $(P\wedge Q)\vee(P\wedge\neg Q)\Leftrightarrow P\wedge(Q\vee\neg Q)\Leftrightarrow P\wedge\mathbf{T}\Leftrightarrow P$

例题 9 证明 $P\rightarrow(Q\rightarrow R)\Leftrightarrow Q\rightarrow(P\rightarrow R)\Leftrightarrow\neg R\rightarrow(Q\rightarrow\neg P)$

证明 $P\rightarrow(Q\rightarrow R)\Leftrightarrow\neg P\vee(\neg Q\vee R)\Leftrightarrow\neg Q\vee(\neg P\vee R)$

$\Leftrightarrow Q\rightarrow(P\rightarrow R)$

又， $P\rightarrow(Q\rightarrow R)\Leftrightarrow\neg P\vee(\neg Q\vee R)\Leftrightarrow R\vee(\neg Q\vee\neg P)$

$\Leftrightarrow\neg R\rightarrow(Q\rightarrow\neg P)$

例题 10 证明 $((P\vee Q)\wedge\neg(\neg P\wedge(\neg Q\vee\neg R)))$

$\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge\neg R)\Leftrightarrow\mathbf{T}$

证明 原式左边$\Leftrightarrow((P\vee Q)\wedge\neg(\neg P\wedge\neg(Q\wedge R)))$

$\vee\neg(P\vee Q)\vee\neg(P\vee R)$

$\Leftrightarrow((P\vee Q)\wedge(P\vee(Q\wedge R)))\vee\neg(P\vee Q)\vee\neg(P\vee R)$

$\Leftrightarrow((P\vee Q)\wedge((P\vee Q)\wedge(P\vee R)))$

$\vee\neg((P\vee Q)\wedge(P\vee R))$

$\Leftrightarrow((P\vee Q)\wedge(P\vee R))\vee\neg((P\vee Q)\wedge(P\vee R))$

$\Leftrightarrow\mathbf{T}$

1-4 习题

(1) 求下列各复合命题的真值表。

a) $P\rightarrow(Q\vee R)$

b) $(P\vee R)\wedge(P\rightarrow Q)$

c) $(P\vee Q)\rightleftarrows(Q\vee P)$

d) $(P\vee\neg Q)\wedge R$

e) $(P\rightarrow(Q\rightarrow R))\rightarrow((P\rightarrow Q)\rightarrow(P\rightarrow R))$

(2) 试求下列各命题的真值表并解释其结果。

a) $(P \to Q) \wedge (Q \to P)$

b) $(P \wedge Q) \to P$

c) $Q \to (P \vee Q)$

d) $(P \to Q) \rightleftarrows (\neg P \vee Q)$

e) $(\neg P \vee Q) \wedge (\neg(P \wedge \neg Q))$

(3) 作出下列命题的真值表: 并非"室内很冷或很乱"也不是"室外暖和且室内太脏"。

(4) 试以真值表证明下列命题。

a) 合取运算之结合律;

b) 析取运算之结合律;

c) 合取($\wedge$)对析取($\vee$)之分配律;

d) 德·摩根律。

(5) 由下表求出公式 F_1, F_2, F_3, F_4, F_5, F_6。在表上有问号(?)的地方以 **F** 或 **T** 代入都可以,只要所求的公式形式较为简单。

表 1-4.11

P	Q	R	F_1	F_2	F_3	F_4	F_5	F_6
T	**T**	**T**	**T**	**F**	**T**	**T**	**F**	?
T	**T**	**F**	**F**	**F**	**T**	**F**	**F**	?
T	**F**	**T**	**T**	**F**	**F**	**T**	**T**	?
T	**F**	**F**	**F**	**T**	**F**	**T**	?	?
F	**T**	**T**	**T**	**F**	**F**	**T**	**T**	**F**
F	**T**	**F**	**T**	**F**	**F**	**F**	**T**	**F**
F	**F**	**T**	**T**	**F**	**T**	**T**	?	**F**
F	**F**	**F**	**F**	**T**	**F**	**T**	?	**T**

(6) 下表为含有两个变元的命题公式的各种情况真值表,对于每一列,试写出一个至多包含此两个变元的命题公式。

表 1-4.12

P	Q	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
F	**F**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**
F	**T**	**F**	**F**	**T**	**T**	**F**	**F**	**T**	**T**	**F**	**F**	**T**	**T**	**F**	**F**	**T**	**T**
T	**F**	**F**	**F**	**F**	**F**	**T**	**T**	**T**	**T**	**F**	**F**	**F**	**F**	**T**	**T**	**T**	**T**
T	**T**	**F**	**F**	**F**	**F**	**F**	**F**	**F**	**F**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**T**

(7) 证明下列等价式。

a) $A \to (B \to A) \Leftrightarrow \neg A \to (A \to \neg B)$

b) $\neg(A \rightleftarrows B) \Leftrightarrow (A \vee B) \wedge \neg(A \wedge B)$

c) $\neg(A \to B) \Leftrightarrow A \wedge \neg B$

d) $\neg(A \rightleftarrows B) \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)$

e) $(((A \wedge B \wedge C) \to D) \wedge (C \to (A \vee B \vee D))) \Leftrightarrow ((C \wedge (A \rightleftarrows B)) \to D)$

f) $A \to (B \vee C) \Leftrightarrow (A \wedge \neg B) \to C$

g) $(A \to D) \wedge (B \to D) \Leftrightarrow (A \vee B) \to D$

h) $((A \wedge B) \to C) \wedge (B \to (D \vee C)) \Leftrightarrow (B \wedge (D \to A)) \to C$

(8) 化简以下各式。

a) $((A \to B) \rightleftarrows (\neg B \to \neg A)) \wedge C$

b) $A \vee (\neg A \vee (B \wedge \neg B))$

c) $(A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C)$

(9) 如果 $A \vee C \Leftrightarrow B \vee C$, 是否有 $A \Leftrightarrow B$? 如果 $A \wedge C \Leftrightarrow B \wedge C$ 是否有 $A \Leftrightarrow B$? 如果 $\neg A \Leftrightarrow \neg B$ 是否有 $A \Leftrightarrow B$?

1-5 重言式与蕴含式

从上节真值表和命题的等价公式推证中可以看到，有些命题公式，无论对分量作何种指派，其对应的真值都为 $\boldsymbol{T}$ 或都为 $\boldsymbol{F}$，这两类特殊的命题公式在今后的命题演算中极为有用。为此，下面作较详细的讨论。

定义 1-5.1 给定一命题公式，若无论对分量作怎样的指派，其对应的真值永为 $\boldsymbol{T}$，则称该命题公式为**重言式**或**永真公式**。

定义 1-5.2 给定一命题公式，若无论对分量作怎样的指派，其对应的真值永为 $\boldsymbol{F}$，则称该命题为矛盾式或永假公式。

定理 1-5.1 任何两个重言式的合取或析取，仍然是一个重言式。

证明　设 A 和 B 为两个重言式，则不论 A 和 B 的分量指派任何真值，总有 A 为 $\boldsymbol{T}$，B 为 $\boldsymbol{T}$，故 $A \wedge B \Leftrightarrow \boldsymbol{T}$，$A \vee B \Leftrightarrow \boldsymbol{T}$。 □

定理 1-5.2 一个重言式，对同一分量都用任何合式公式置

换，其结果仍为一重言式。

证明 由于重言式的真值与分量的指派无关，故对同一分量以任何合式公式置换后，重言式的真值仍永为 $\boldsymbol{T}$。 □

对于矛盾式也有类似于定理 1-5.1 和定理 1-5.2 的结果。

例题 1 证明 $((P\lor S)\land R)\lor\neg((P\lor S)\land R)$为重言式。

证明 因为 $P\lor\neg P\Leftrightarrow T$，如以$((P\lor S)\land R)$置换 P 即得

$$((P\lor S)\land R)\lor\neg((P\lor S)\land R)\Leftrightarrow T$$

定理 1-5.3 设 A、B 为两个命题公式，$A\Leftrightarrow B$ 当且仅当 $A\rightleftarrows B$ 为一个重言式。

证明 若 $A\Leftrightarrow B$，则 A、B 有相同真值，即 $A\rightleftarrows B$ 永为 $\boldsymbol{T}$。

若 $A\rightleftarrows B$ 为重言式，则 $A\rightleftarrows B$ 永为 $\boldsymbol{T}$，故 A、B 的真值相同，即 $A\Leftrightarrow B$。 □

例题 2 证明 $\neg(P\land Q)\Leftrightarrow(\neg P\lor\neg Q)$

证明 由上节例题 4 中表 1-4.4 可知，$\neg(P\land Q)\rightleftarrows(\neg P\lor\neg Q)$为重言式，故据定理 1-5.3：

$$\neg(P\land Q)\Leftrightarrow(\neg P\lor\neg Q)$$

我们知道，联结词 $\rightleftarrows$ 可以用 $\rightarrow$ 来表达。即：

$$A\rightleftarrows B\Leftrightarrow(A\rightarrow B)\land(B\rightarrow A)$$

下面讨论 $A\rightarrow B$ 的重言式。

定义 1-5.3 当且仅当 $P\rightarrow Q$ 是一个重言式时，我们称“P 蕴含 Q”，并记作 $P\Rightarrow Q$。

因为 $P\rightarrow Q$ 不是对称的，即 $P\rightarrow Q$ 与 $Q\rightarrow P$ 不等价，对 $P\rightarrow Q$ 来说，$Q\rightarrow P$ 称作它的逆换式；$\neg P\rightarrow\neg Q$ 称为它的反换式；$\neg Q\rightarrow\neg P$ 称它的逆反式，它们之间的关系如表 1-5.1 所示。

从表 1-5.1 中看出：$(P\rightarrow Q)\Leftrightarrow(\neg Q\rightarrow\neg P)$

$$(Q\rightarrow P)\Leftrightarrow(\neg P\rightarrow\neg Q)$$

因此要证明 $P\Rightarrow Q$，只需证明 $\neg Q\Rightarrow\neg P$，反之亦然。要证 $P\Rightarrow Q$，即证 $P\rightarrow Q$ 是重言式。对于 $P\rightarrow Q$ 来说，除 P 的真值取 $\boldsymbol{T}$，Q 的真值取 $\boldsymbol{F}$ 这样一种指派时，$P\rightarrow Q$ 的真值为 $\boldsymbol{F}$ 外，其余情

表 1-5.1

P	Q	$\neg P$	$\neg Q$	$P\to Q$	$\neg Q\to\neg P$	$Q\to P$	$\neg P\to\neg Q$
T	**T**	**F**	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**	**T**	**T**
F	**T**	**T**	**F**	**T**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**	**T**	**T**	**T**

况，$P\to Q$ 的真值为 **T**。故要证 $P\Rightarrow Q$，只需对条件命题 $P\to Q$ 的前件 P，指定真值为 **T**，若由此推出 Q 的真值亦为 **T**，则 $P\to Q$ 是重言式，即 $P\Rightarrow Q$ 成立；同理，如对条件命题 $P\to Q$ 中，假定后件 Q 的真值取 **F**，若由此推出 P 的真值为 **F**，即推证了 $\neg Q\Rightarrow\neg P$，故 $P\Rightarrow Q$ 成立。

例题 1 推证 $\neg Q\wedge(P\to Q)\Rightarrow\neg P$

证法 1 假定 $\neg Q\wedge(P\to Q)$ 为 **T**，则 $\neg Q$ 为 **T**，且 $(P\to Q)$ 为 **T**。由 Q 为 **F**，$P\to Q$ 为 **T**，则必须 P 为 **F**，故 $\neg P$ 为 **T**。

证法 2 假定 $\neg P$ 为 **F**，则 P 为 **T**。

(a)：若 Q 为 **F**，则 $P\to Q$ 为 **F**，$\neg Q\wedge(P\to Q)$ 为 **F**。

(b)：若 Q 为 **T**，则 $\neg Q$ 为 **F**，$\neg Q\wedge(P\to Q)$ 为 **F**。

所以 $\neg Q\wedge(P\to Q)\Rightarrow\neg P$ 成立。

表 1-5.2 所列各蕴含式都可如上述推理方法证明：

表 1-5.2

$P\wedge Q\Rightarrow P$	1
$P\wedge Q\Rightarrow Q$	2
$P\Rightarrow P\vee Q$	3
$\neg P\Rightarrow P\to Q$	4
$Q\Rightarrow P\to Q$	5
$\neg(P\to Q)\Rightarrow P$	6
$\neg(P\to Q)\Rightarrow\neg Q$	7
$P\wedge(P\to Q)\Rightarrow Q$	8
$\neg Q\wedge(P\to Q)\Rightarrow\neg P$	9
$\neg P\wedge(P\vee Q)\Rightarrow Q$	10
$(P\to Q)\wedge(Q\to R)\Rightarrow P\to R$	11
$(P\vee Q)\wedge(P\to R)\wedge(Q\to R)\Rightarrow R$	12
$(P\to Q)\wedge(R\to S)\Rightarrow(P\wedge R)\to(Q\wedge S)$	13
$(P\rightleftarrows Q)\wedge(Q\rightleftarrows R)\Rightarrow(P\rightleftarrows R)$	14

就象联结词 $\rightleftarrows$ 和 $\rightarrow$ 的关系一样，等价式与蕴含式之间也有紧密的联系。

定理 1-5.4 设 P、Q 为任意两个命题公式，$P\Leftrightarrow Q$ 的充分必要条件是 $P\Rightarrow Q$ 且 $Q\Rightarrow P$。

证明 若 $P\Leftrightarrow Q$，则 $P\rightleftarrows Q$ 为重言式，因为 $P\rightleftarrows Q\Leftrightarrow(P\rightarrow Q)\wedge(Q\rightarrow P)$，故 $P\rightarrow Q$ 为 $\boldsymbol{T}$ 且 $Q\rightarrow P$ 为 $\boldsymbol{T}$，即 $P\Rightarrow Q$，$Q\Rightarrow P$ 成立。反之，若 $P\Rightarrow Q$ 且 $Q\Rightarrow P$，则 $P\rightarrow Q$ 为 $\boldsymbol{T}$ 且 $Q\rightarrow P$ 为 $\boldsymbol{T}$，因此 $P\rightleftarrows Q$ 为 $\boldsymbol{T}$，$P\rightleftarrows Q$ 是重言式，即 $P\Leftrightarrow Q$。 □

这个定理也可作为两个公式等价的定义。

蕴含有下面几个常用的性质：

(1) 设 A、B、C 为合式公式，若 $A\Rightarrow B$ 且 A 是重言式，则 B 必是重言式。

证明 因为 $A\rightarrow B$ 永为 $\boldsymbol{T}$，所以，当 A 为 $\boldsymbol{T}$ 时，B 必永为 $\boldsymbol{T}$。

(2) 若 $A\Rightarrow B$，$B\Rightarrow C$，则 $A\Rightarrow C$，即蕴含关系是传递的。

证明 由 $A\Rightarrow B$，$B\Rightarrow C$，即 $A\rightarrow B$，$B\rightarrow C$ 为重言式。所以 $(A\rightarrow B)\wedge(B\rightarrow C)$ 为重言式。

由表 1-5.2 的 (11) 式，$(A\rightarrow B)\wedge(B\rightarrow C)\Rightarrow A\rightarrow C$，故由性质(1)，$A\rightarrow C$ 为重言式，即 $A\Rightarrow C$。

(3) 若 $A\Rightarrow B$，且 $A\Rightarrow C$，那末 $A\Rightarrow(B\wedge C)$。

证明 由假设 $A\rightarrow B$，$A\rightarrow C$ 为重言式。设 A 为 $\boldsymbol{T}$，则 B、C 为 $\boldsymbol{T}$，故 $B\wedge C$ 为 $\boldsymbol{T}$。因此，$A\rightarrow(B\wedge C)$ 为 $\boldsymbol{T}$。

若 A 为 $\boldsymbol{F}$，则 $B\wedge C$ 不论有怎样的真值，$A\rightarrow(B\wedge C)$ 为 $\boldsymbol{T}$。所以，

$$A\Rightarrow(B\wedge C)$$

(4) 若 $A\Rightarrow B$ 且 $C\Rightarrow B$，则 $A\vee C\Rightarrow B$。

证明 因为 $A\rightarrow B$ 为 $\boldsymbol{T}$，$C\rightarrow B$ 为 $\boldsymbol{T}$，故 $(\neg A\vee B)\wedge(\neg C\vee B)$ 为 $\boldsymbol{T}$。

即 $(\neg A\wedge\neg C)\vee B$ 为 T 或 $A\vee C\rightarrow B$ 为 $\boldsymbol{T}$。

所以

$$A\vee C\Rightarrow B$$

1-5 习题

(1) 试证下列各式为重言式。

a) $(P\wedge(P\rightarrow Q))\rightarrow Q$

b) $\neg P\rightarrow(P\rightarrow Q)$

c) $((P\rightarrow Q)\wedge(Q\rightarrow R))\rightarrow(P\rightarrow R)$

d) $((a\wedge b)\vee(b\wedge c)\vee(c\wedge a))\rightleftarrows(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$

(2) 不构造真值表证明下列蕴含式。

a) $(P\rightarrow Q)\Rightarrow P\rightarrow(P\wedge Q)$

b) $(P\rightarrow Q)\rightarrow Q\Rightarrow P\vee Q$

c) $(Q\rightarrow(P\wedge\neg P))\rightarrow(R\rightarrow(R\rightarrow(P\wedge\neg P)))\Rightarrow R\rightarrow Q$

(3) 设 P 表示命题"8 是偶数"，Q 表示命题"糖果是甜的"。试以句子写出

a) $P\rightarrow Q$

b) a)的逆换式

c) a)的反换式

d) a)的逆反式

(4) 叙述下列各个命题的逆换式和逆反式，并以符号写出。

a) 如果天下雨，我不去。

b) 仅当你走我将留下。

c) 如果我不能获得更多帮助，我不能完成这个任务。

(5) 试证明 $P\rightleftarrows Q$，Q 逻辑蕴含 P。

(6) 检验下述论证的有效性。

如果我学习，那么我数学不会不及格。

如果我不热衷于玩扑克，那么我将学习。

但我数学不及格。

因此我热衷于玩扑克。

(7) 用符号写出下列各式并且验证论证的有效性。

如果 6 是偶数，则 7 被 2 除不尽。

或 5 不是素数，或 7 被 2 除尽。

但 5 是素数。

所以 6 是奇数。

(8) 逻辑推证以下各式。

a) $P\Rightarrow(\neg P\rightarrow Q)$

b) $\neg A\wedge B\wedge A\Rightarrow C$

c) $C \Rightarrow A \vee B \vee \neg B$

d) $\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$

e) $\neg A \rightarrow (B \vee C)$, $D \vee E$, $(D \vee E) \rightarrow \neg A \Rightarrow B \vee C$

f) $(A \wedge B) \rightarrow C$, $\neg D$, $\neg C \vee D \Rightarrow \neg A \vee \neg B$

(9) 求与下列命题等价的逆反式。

a) 如果他有勇气，他将得胜。

b) 仅当他不累他将得胜。

1-6 其他联结词

我们已经定义了联结词 $\neg$, $\wedge$, $\vee$, $\rightarrow$ 和 $\rightleftarrows$, 但这些联结词还不能很广泛地直接表达命题间的联系，为此我们再定义一些命题联结词。

定义 1-6.1 设 P 和 Q 是两个命题公式，复合命题 $P \overline{\vee} Q$ 称作 P 和 Q 的不可兼析取。$P \overline{\vee} Q$ 的真值为 $\boldsymbol{T}$，当且仅当 P 与 Q 的真值不相同时为 $\boldsymbol{T}$，否则，$P \overline{\vee} Q$ 的真值为 $\boldsymbol{F}$。

联结词"$\overline{\vee}$"的定义如表 1-6.1 所示。

表 1-6.1

P	Q	$P \overline{\vee} Q$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

从上述定义可知联结词"$\overline{\vee}$"有以下性质：

设 P、Q、R 为命题公式，则有

(1) $P \overline{\vee} Q \Leftrightarrow Q \overline{\vee} P$

(2) $(P \overline{\vee} Q) \overline{\vee} R \Leftrightarrow P \overline{\vee} (Q \overline{\vee} R)$

(3) $P \wedge (Q \overline{\vee} R) \Leftrightarrow (P \wedge Q) \overline{\vee} (P \wedge R)$

(4) $(P \overline{\vee} Q) \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q)$

(5) $(P \overline{\vee} Q) \Leftrightarrow \neg(P \rightleftarrows Q)$

(6) $P\overline{\vee}P\Leftrightarrow \boldsymbol{F}$, $\boldsymbol{F}\overline{\vee}P\Leftrightarrow P$, $\boldsymbol{T}\overline{\vee}P\Leftrightarrow \neg P$。

定理 1-6.1 设 P、Q、R 为命题公式。如果 $P\overline{\vee}Q\Leftrightarrow R$，则 $P\overline{\vee}R\Leftrightarrow Q$, $Q\overline{\vee}R\Leftrightarrow P$，且 $P\overline{\vee}Q\overline{\vee}R$ 为一矛盾式。

证明 如果 $P\overline{\vee}Q\Leftrightarrow R$,

则 $P\overline{\vee}R\Leftrightarrow P\overline{\vee}P\overline{\vee}Q\Leftrightarrow \boldsymbol{F}\overline{\vee}Q\Leftrightarrow Q$

$Q\overline{\vee}R\Leftrightarrow Q\overline{\vee}P\overline{\vee}Q\Leftrightarrow \boldsymbol{F}\overline{\vee}P\Leftrightarrow P$

$P\overline{\vee}Q\overline{\vee}R\Leftrightarrow R\overline{\vee}R\Leftrightarrow \boldsymbol{F}$ □

定义 1-6.2 设 P 和 Q 是两个命题公式，复合命题 $P\overset{c}{\rightarrow}Q$ 称作命题 P 和 Q 的条件否定，$P\overset{c}{\rightarrow}Q$ 的真值为 $\boldsymbol{T}$，当且仅当 P 的真值为 $\boldsymbol{T}$，Q 的真值为 $\boldsymbol{F}$，否则，$P\overset{c}{\rightarrow}Q$ 的真值为 $\boldsymbol{F}$。

联结词"$\overset{c}{\rightarrow}$"的定义如表 1-6.2 所示。

表 1-6.2

P	Q	$P\overset{c}{\rightarrow}Q$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{T}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{F}$

从定义可知 $P\overset{c}{\rightarrow}Q\Leftrightarrow \neg(P\rightarrow Q)$。

在计算机设计中，经常应用另外二个联结词。

定义 1-6.3 设 P 和 Q 是两个命题公式，复合命题 $P\uparrow Q$ 称作 P 和 Q 的"与非"。当且仅当 P 和 Q 的真值都是 $\boldsymbol{T}$ 时，$P\uparrow Q$ 为 $\boldsymbol{F}$，否则 $P\uparrow Q$ 的真值都为 $\boldsymbol{T}$。

联结词"$\uparrow$"的定义如表 1-6.3 所示。

表 1-6.3

P	Q	$P\uparrow Q$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{T}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{T}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{T}$

从上表可以看出 $P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$，故联结词“↑”可称为“与非”。

联结词“↑”有如下几个性质：

(1) $P \uparrow P \Leftrightarrow \neg(P \wedge P) \Leftrightarrow \neg P$

(2) $(P \uparrow Q) \uparrow (P \uparrow Q) \Leftrightarrow \neg(P \uparrow Q) \Leftrightarrow P \wedge Q$

(3) $(P \uparrow P) \uparrow (Q \uparrow Q) \Leftrightarrow \neg P \uparrow \neg Q \Leftrightarrow \neg(\neg P \wedge \neg Q) \Leftrightarrow P \vee Q$

定义 1-6.4 设 P 和 Q 是两个命题公式，复合命题 $P \downarrow Q$ 称作 P 和 Q 的“或非”，当且仅当 P 和 Q 的真值都为 $\boldsymbol{F}$ 时，$P \downarrow Q$ 的真值为 $\boldsymbol{T}$，否则 $P \downarrow Q$ 的真值都为 $\boldsymbol{F}$。

联结词“↓”的定义如表 1-6.4 所示。

表 1-6.4

P	Q	$P \downarrow Q$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{T}$

从上表可以看出 $P \downarrow Q \Leftrightarrow \neg(P \vee Q)$，故联结词“↓”可称作“或非”。

联结词“↓”有如下几个性质：

(1) $P \downarrow P \Leftrightarrow \neg(P \vee P) \Leftrightarrow \neg P$

(2) $(P \downarrow Q) \downarrow (P \downarrow Q) \Leftrightarrow \neg(P \downarrow Q) \Leftrightarrow P \vee Q$

(3) $(P \downarrow P) \downarrow (Q \downarrow Q) \Leftrightarrow \neg P \downarrow \neg Q \Leftrightarrow P \wedge Q$

对于包含$\overline{\vee}$，$\xrightarrow{c}$，↑，↓ 的复合命题，其合式公式类似于定义 1-3.1。

至此，我们一共介绍了九个联结词，是否还需要定义其它联结词呢？

我们知道，命题联结词在命题演算中是通过真值表定义的，两个命题变元，恰可构成 2^4 个不等价的命题公式，如表 1-6.5 所示。

表 1-6.5

P	Q	联结词 1	联结词 2	联结词 3	联结词 4	联结词 5	联结词 6	联结词 7	联结词 8
T	T	T	F	T	T	F	F	T	F
T	F	T	F	T	F	F	T	F	T
F	T	T	F	F	T	T	F	F	T
F	F	T	F	F	F	T	T	F	T

P	Q	联结词 9	联结词 10	联结词 11	联结词 12	联结词 13	联结词 14	联结词 15	联结词 16
T	T	T	F	T	F	T	F	T	F
T	F	T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T	F	T
F	F	F	T	T	F	T	F	T	F

从上表中可以看出：

第 1、2 列分别表示永真 $\boldsymbol{T}$ 及永假 $\boldsymbol{F}$；

第 3、4 列分别表示命题变元 P、Q；

第 5、6 列分别表示命题变元的否定：$\neg P$，$\neg Q$；

第 7 列表示“合取”命题：$P\wedge Q$；

第 8 列表示“与非”命题：$P\uparrow Q$；

第 9 列表示“析取”命题：$P\vee Q$；

第 10 列表示“或非”命题：$P\downarrow Q$；

第 11、15 列分别表示条件命题：$P\rightarrow Q$，$Q\rightarrow P$；

第 12、16 列分别表示逆条件命题：$P\overset{c}{\rightarrow}Q$，$Q\overset{c}{\rightarrow}P$；

第 13 列表示双条件命题：$P\rightleftarrows Q$；

第 14 列表示不可兼析取命题：$P\overline{\vee}Q$。

由上述分析，除常量 $\boldsymbol{T}$、$\boldsymbol{F}$ 及命题变元本身外，命题联结词一共有九个就够了。

虽然我们定义了上述九个联结词，但这些联结词并非都是必要的，因为包含某些联结词的公式可以用另外一些联结词的公式

等价代换。现在考虑最小联结词组，对于任何一个命题公式，都能由仅含这些联结词的命题公式等价代换。这是因为

(1) 由 $(P \rightleftarrows Q) \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$，故可把包含“$\rightleftarrows$”的公式等价变换为包含“$\wedge$”和“$\rightarrow$”的公式。

(2) 由 $P \rightarrow Q \Leftrightarrow \neg P \vee Q$，说明包含“$\rightarrow$”的公式可以变换为包含“$\neg$”和“$\vee$”的公式。

(3) 由 $P \wedge Q \Leftrightarrow \neg(\neg P \vee \neg Q)$，$P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$，说明“$\wedge$”和“$\vee$”可以相互代换。

故由“$\neg$”、“$\wedge$”、“$\vee$”、“$\rightarrow$”、“$\rightleftarrows$”这五个联结词组成的命题公式，必可由$\{\neg, \vee\}$或$\{\neg, \wedge\}$组成的命题公式所替代。

对于其他一些联结词，根据定义及有关性质有：

$$(P \overline{\vee} Q) \Leftrightarrow \neg(P \rightleftarrows Q)$$

$$P \stackrel{c}{\rightarrow} Q \Leftrightarrow \neg(P \rightarrow Q)$$

$$P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$$

$$P \downarrow Q \Leftrightarrow \neg(P \vee Q)$$

故任意命题公式都可由仅包含$\{\neg, \vee\}$或$\{\neg, \wedge\}$的命题公式等价代换。所需注意的是上述联结词组$\{\neg, \vee\}$和$\{\neg, \wedge\}$不能再归为$\{\neg\}$，$\{\vee\}$，$\{\wedge\}$或$\{\vee, \wedge\}$。因为从合式公式定义可以看出包含二元联结词的命题公式不能用仅包含一元联结词的命题公式等价代换，同时如有

$$\neg P \Leftrightarrow (\cdots(P \wedge R) \vee \cdots \wedge \cdots)$$

的形式，则对该等价式右边所出现的变元，都指派真值 $\boldsymbol{T}$，由于 $\wedge$ 和 $\vee$ 的各次复合结果，其真值必为 $\boldsymbol{T}$，而该式的左边的真值为 $\boldsymbol{F}$，产生矛盾，说明“$\neg$”是不能由“$\vee$”或“$\wedge$”的复合所替代，故最小联结词组应为$\{\neg, \vee\}$或$\{\neg, \wedge\}$。

当然，由联结词“$\uparrow$”和联结词“$\downarrow$”的性质，可知联结词“$\neg$”、“$\wedge$”和“$\vee$”可分别用“$\uparrow$”或“$\downarrow$”所替代，故最小联结词组亦可为$\{\uparrow\}$或$\{\downarrow\}$。

1-6 习题

(1) 把下列各式用只含 $\vee$ 和 $\neg$ 的等价式表达，并要尽可能的简单。

a) $(P\wedge Q)\wedge\neg P$

b) $(P\rightarrow(Q\vee\neg R))\wedge\neg P\wedge Q$

c) $\neg P\wedge\neg Q\wedge(\neg R\rightarrow P)$

(2) 对下列各式仅用“或非”($\downarrow$)表达。

a) $\neg P$

b) $P\vee Q$

c) $P\wedge Q$

(3) 把 $P\rightarrow(\neg P\rightarrow Q)$ 表示为只含有“$\uparrow$”的等价公式，把同样的公式表示为只含有“$\downarrow$”的等价公式。

(4) 把 $P\uparrow Q$ 表示为只含有“$\downarrow$”的等价公式。

(5) 证明 $\neg(B\uparrow C)\Leftrightarrow\neg B\downarrow\neg C$

$\neg(B\downarrow C)\Leftrightarrow\neg B\uparrow\neg C$

(6) 联结词“$\uparrow$”和“$\downarrow$”服从结合律吗?

*(7) 证明 $\{\rightleftarrows,\neg\}$ 和 $\{\overline{\vee},\neg\}$不是最小联结词组。

(8) 证明$\{\vee\}$，$\{\wedge\}$和$\{\rightarrow\}$不是最小联结词组。

(9) 证明$\{\neg,\rightarrow\}$和$\{\neg,\overset{c}{\rightarrow}\}$是最小联结词组。

1-7 对偶与范式

从上节可看到命题公式的最小联结词组为$\{\neg,\vee\}$或$\{\neg,\wedge\}$，但实际上为了使用方便，命题公式常常同时包含$\{\neg,\vee,\wedge\}$。我们从表 1-4.8 可以看到命题定律除对合律外都是成对出现的，其不同的只是 $\vee$ 和 $\wedge$ 互换。我们把这样的公式称作具有对偶规律。

定义 1-7.1 在给定的命题公式中，将联结词 $\vee$ 换成 $\wedge$，将 $\wedge$ 换成 $\vee$，若有特殊变元 $\boldsymbol{F}$ 和 $\boldsymbol{T}$ 亦相互取代，所得公式 A^* 称为 A 的对偶式。

显然 A 也是 A^* 的对偶式。

例题 1 写出下列表达式的对偶式

(a) $(P\vee Q)\wedge R$

(b) $(P\wedge Q)\vee \mathbf{T}$

(c) $\neg(P\vee Q)\wedge(P\vee\neg(Q\wedge\neg S))$

解　这些表达式的对偶式是:

(a) $(P\wedge Q)\vee R$

(b) $(P\vee Q)\wedge \mathbf{F}$

(c) $\neg(P\wedge Q)\vee(P\wedge\neg(Q\vee\neg S))$

例题 2　求 $P\uparrow Q$, $P\downarrow Q$ 的对偶式。

解　因为 $P\uparrow Q\Leftrightarrow\neg(P\wedge Q)$，故 $P\uparrow Q$ 的对偶式为 $\neg(P\vee Q)$，即 $P\downarrow Q$。同理 $P\downarrow Q$ 的对偶式是 $P\uparrow Q$。

定理 1-7.1　设 A 和 A^* 是对偶式，P_1, P_2, …, P_n 是出现在 A 和 A^* 中的原子变元，则

$$\neg A(P_1, P_2, \cdots, P_n)\Leftrightarrow A^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$$

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n)\Leftrightarrow\neg A^*(P_1, P_2, \cdots, P_n)$$

证明　由德·摩根定律

$$P\wedge Q\Leftrightarrow\neg(\neg P\vee\neg Q), \quad P\vee Q\Leftrightarrow\neg(\neg P\wedge\neg Q)$$

故

$$\neg A(P_1, P_2, \cdots, P_n)\Leftrightarrow A^*(\neg P_1, \neg P_2, \cdots, \neg P_n)$$

同理

$$\neg A^*(P_1, P_2, \cdots, P_n)\Leftrightarrow A(\neg P_1, \neg P_2, \cdots, \neg P_n)$$ □

例题 3　设 $A^*(S, W, R)$ 是 $\neg S\wedge(\neg W\vee R)$，证明

$$A^*(\neg S, \neg W, \neg R)\Leftrightarrow\neg A(S, W, R)$$

证明　由于 $A^*(S, W, R)$ 是 $\neg S\wedge(\neg W\vee R)$，则 $A^*(\neg S, \neg W, \neg R)$ 是 $S\wedge(W\vee\neg R)$。但 $A(S, W, R)$ 是 $\neg S\vee(\neg W\wedge R)$，故 $\neg A(S, W, R)$ 是 $\neg(\neg S\vee(\neg W\wedge R))\Leftrightarrow S\wedge(W\vee\neg R)$。

所以　$$A^*(\neg S, \neg W, \neg R)\Leftrightarrow\neg A(S, W, R)$$

定理 1-7.2　设 P_1, P_2, …, P_n 是出现在公式 A 和 B 中的所有原子变元，如果 $A\Leftrightarrow B$，则 $A^*\Leftrightarrow B^*$。

证明　因为 $A\Leftrightarrow B$，即

$$A(P_1, P_2, \cdots, P_n)\rightleftarrows B(P_1, P_2, \cdots, P_n)$$

是一个重言式，故

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n)\rightleftarrows B(\neg P_1, \neg P_2, \cdots, \neg P_n)$$

也是一个重言式。即

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow B(\neg P_1, \neg P_2, \cdots, \neg P_n)$$

由定理 1-7.1 得

$$\neg A^*(P_1, P_2, \cdots, P_n) \Leftrightarrow \neg B^*(P_1, P_2, \cdots, P_n)$$

因此 $$A^* \Leftrightarrow B^*$$ □

例题 4 如果 $A(P, Q, R)$ 是 $P \uparrow (Q \wedge \neg(R \downarrow P))$，求它的对偶式 $A^*(P, Q, R)$。并求与 A 及 A^* 等价，但仅包含联结词"$\wedge$"、"$\vee$"及"$\neg$"的公式。

解 因 $A(P, Q, R)$ 是 $P \uparrow (Q \wedge \neg(R \downarrow P))$

故 $A^*(P, Q, R)$ 是 $P \downarrow (Q \vee \neg(R \uparrow P))$

但 $P \uparrow (Q \wedge \neg(R \downarrow P)) \Leftrightarrow \neg(P \wedge (Q \wedge (R \vee P)))$

所以 $P \downarrow (Q \vee \neg(R \uparrow P)) \Leftrightarrow \neg(P \vee (Q \vee (R \wedge P)))$

从真值表和对偶律等可以简化或推证一些命题公式。同一命题公式可以有各种相互等价的表达形式，为了把命题公式规范化，下面讨论命题公式的范式问题。

定义 1-7.2 一个命题公式称为合取范式，当且仅当它具有型式：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n, \quad (n \geqslant 1)$$

其中 $A_1, A_2, \cdots, A_n$ 都是由命题变元或其否定所组成的析取式。

例如 $(P \vee \neg Q \vee R) \wedge (\neg P \vee Q) \wedge \neg Q$ 是一个合取范式。

定义 1-7.3 一个命题公式称为析取范式，当且仅当它具有型式：

$$A_1 \vee A_2 \vee \cdots \vee A_n, \quad (n \geqslant 1)$$

其中 $A_1, A_2, \cdots, A_n$ 都是由命题变元或其否定所组成的合取式。

例如 $\neg P \vee (P \wedge Q) \vee (P \wedge \neg Q \wedge R)$ 是析取范式。

任何一个命题公式，求它的合取范式或析取范式，可以通过下面三个步骤进行：

(1) 将公式中的联结词化归成 $\wedge$，$\vee$ 及 $\neg$。

(2) 利用德·摩根律将否定符号 $\neg$ 直接移到各个命题变元之前。

(3) 利用分配律、结合律将公式归约为合取范式或析取范式。

例题5 求$(P\wedge(Q\to R))\to S$的合取范式。

解 $(P\wedge(Q\to R))\to S\Leftrightarrow(P\wedge(\neg Q\vee R))\to S$

$\Leftrightarrow\neg(P\wedge(\neg Q\vee R))\vee S\Leftrightarrow\neg P\vee(Q\wedge\neg R)\vee S$

$\Leftrightarrow(\neg P\vee S)\vee(Q\wedge\neg R)$

$\Leftrightarrow(\neg P\vee S\vee Q)\wedge(\neg P\vee S\vee\neg R)$

例题6 求$\neg(P\vee Q)\rightleftarrows(P\wedge Q)$的析取范式。

解 因为有公式

$$(A\rightleftarrows B)\Leftrightarrow(A\wedge B)\vee(\neg A\wedge\neg B)$$

故 $\neg(P\vee Q)\rightleftarrows(P\wedge Q)\Leftrightarrow(\neg(P\vee Q)\wedge(P\wedge Q))\vee((P\vee Q)\wedge\neg(P\wedge Q))$

$\Leftrightarrow(\neg P\wedge\neg Q\wedge P\wedge Q)\vee((P\vee Q)\wedge(\neg P\vee\neg Q))$

$\Leftrightarrow(\neg P\wedge\neg Q\wedge P\wedge Q)\vee(P\wedge\neg P)\vee(Q\wedge\neg P)$

$\vee(P\wedge\neg Q)\vee(Q\wedge\neg Q)$

一个命题公式的合取范式或析取范式并不是唯一的。例如$P\vee(Q\wedge R)$是一个析取范式，但它亦可以写成

$$P\vee(Q\wedge R)\Leftrightarrow(P\vee Q)\wedge(P\vee R)$$

$$\Leftrightarrow(P\wedge P)\vee(P\wedge R)\vee(Q\wedge P)\vee(Q\wedge R)$$

为了使任意一个命题公式，化成唯一的等价命题的标准形式，下面介绍主范式的有关概念。

定义1-7.4 n个命题变元的合取式，称作布尔合取或小项，其中每个变元与它的否定不能同时存在，但两者必须出现且仅出现一次。

例如，两个命题变元P和Q，其小项为：$P\wedge Q$，$P\wedge\neg Q$，$\neg P\wedge Q$，$\neg P\wedge\neg Q$。

三个命题变元P、Q、R，其小项为：$P\wedge Q\wedge R$，$P\wedge Q\wedge\neg R$，$P\wedge\neg Q\wedge R$，$P\wedge\neg Q\wedge\neg R$，$\neg P\wedge Q\wedge R$，$\neg P\wedge Q\wedge\neg R$，$\neg P\wedge\neg Q\wedge R$，$\neg P\wedge\neg Q\wedge\neg R$。

一般说来，n个命题变元共有2^n个小项。

表1-7.1列出两个变元P和Q及其小项的真值表。

从这个真值表中可以看到，没有两个小项是等价的，且每个小项都只对应P和Q的一组真值指派，使得该小项的真值为T。

这个结论可以推广到三个以上的变元情况，并且由此可以作

表 1-7.1

P	Q	$P\wedge Q$	$P\wedge\neg Q$	$\neg P\wedge Q$	$\neg P\wedge\neg Q$
T	T	T	F	F	F
T	F	F	T	F	F
F	T	F	F	T	F
F	F	F	F	F	T

表 1-7.2

P	Q	R	$\neg P\wedge\neg Q\wedge\neg R$	$\neg P\wedge\neg Q\wedge R$	$\neg P\wedge Q\wedge\neg R$	$\neg P\wedge Q\wedge R$
0	0	0	1	0	0	0
0	0	1	0	1	0	0
0	1	0	0	0	1	0
0	1	1	0	0	0	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0
1	1	1	0	0	0	0

P	Q	R	$P\wedge\neg Q\wedge\neg R$	$P\wedge\neg Q\wedge R$	$P\wedge Q\wedge\neg R$	$P\wedge Q\wedge R$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	1	0	0	0
1	0	1	0	1	0	0
1	1	0	0	0	1	0
1	1	1	0	0	0	1

$m_{000}=\neg P\wedge\neg Q\wedge\neg R$　　$m_{100}=P\wedge\neg Q\wedge\neg R$

$m_{001}=\neg P\wedge\neg Q\wedge R$　　$m_{101}=P\wedge\neg Q\wedge R$

$m_{010}=\neg P\wedge Q\wedge\neg R$　　$m_{110}=P\wedge Q\wedge\neg R$

$m_{011}=\neg P\wedge Q\wedge R$　　$m_{111}=P\wedge Q\wedge R$

出一种编码，使 n 个变元的小项可以很快地写出来。现按三个变元为例说明如下。

设 P、Q、R 为三个命题变元，其真值 $\boldsymbol{T}$ 和 $\boldsymbol{F}$ 分别记为"1"和"0"，则小项的真值表如表 1-7.2 所示。

小项有如下几个性质：

(1) 每一个小项当其真值指派与编码相同时，其真值为 $\boldsymbol{T}$，在其余 2^n-1 种指派情况下均为 $\boldsymbol{F}$。

(2) 任意两个不同小项的合取式永假。例如

$$m_{001} \wedge m_{100} = (\neg P \wedge \neg Q \wedge R) \wedge (P \wedge \neg Q \wedge \neg R)$$
$$\Leftrightarrow \neg P \wedge P \wedge \neg Q \wedge R \wedge \neg R \Leftrightarrow \boldsymbol{F}$$

(3) 全体小项的析取式永为真，记为：

$$\sum_{i=0}^{2^n-1} m_i = m_0 \vee m_1 \vee \cdots \vee m_{2^n-1} \Leftrightarrow \boldsymbol{T}$$

定义 1-7.5 对于给定的命题公式，如果有一个等价公式，它仅由小项的析取所组成，则该等价式称作原式的主析取范式。

一个公式的主析取范式可用构成真值表的方法予以写出。

定理 1-7.3 在真值表中，一个公式的真值为 $\boldsymbol{T}$ 的指派所对应的小项的析取，即为此公式的主析取范式。

证明 设给定公式为 A，其真值为 $\boldsymbol{T}$ 的指派所对应的小项为 m_1', m_2', $\cdots$, m_k', 这些小项的析取式记为 B，为此要证 $A \Leftrightarrow B$，即要证 A 与 B 在相应指派下具有相同真值。

首先对 A 为 $\boldsymbol{T}$ 的某一指派，其对应的小项为 m_i'，则因为 m_i' 为 $\boldsymbol{T}$，而 $m_1', m_2', \cdots, m_{i-1}', m_{i+1}', \cdots, m_k'$ 均为 $\boldsymbol{F}$，故 B 为 $\boldsymbol{T}$。

其次，对 A 为 $\boldsymbol{F}$ 的某一指派，其对应的小项不包含在 B 中，即 $m_1', m_2', \cdots, m_k'$ 均为 $\boldsymbol{F}$，故 B 为 $\boldsymbol{F}$。因此，$A \Leftrightarrow B$。 □

例题 6 给定 $P \rightarrow Q$, $P \vee Q$ 和 $\neg(P \wedge Q)$，求这些公式的主析取范式。

解 三公式的真值表如表 1-7.3 所示。故

$$P \rightarrow Q \Leftrightarrow (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge Q)$$
$$P \vee Q \Leftrightarrow (\neg P \wedge Q) \vee (P \wedge \neg Q) \vee (P \wedge Q)$$
$$\neg(P \wedge Q) \Leftrightarrow (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$$

表 1-7.3

P	Q	$P \to Q$	$P \vee Q$	$\neg(P \wedge Q)$
T	**T**	**T**	**T**	**F**
T	**F**	**F**	**T**	**T**
F	**T**	**T**	**T**	**T**
F	**F**	**T**	**F**	**T**

例题 7 设一公式 A 的真值表如表 1-7.4 所示。

表 1-7.4

P	Q	R	A
T	**T**	**T**	**T**
T	**T**	**F**	**F**
T	**F**	**T**	**F**
T	**F**	**F**	**T**
F	**T**	**T**	**F**
F	**T**	**F**	**F**
F	**F**	**T**	**F**
F	**F**	**F**	**T**

求公式 A 的主析取范式。

解：公式 A 的主析取范式为：

$$A \Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R)$$

除了用真值表方法外，也可利用等价公式构成主析取范式。

例题 8 求 $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ 的主析取范式。

解 原式 $\Leftrightarrow (P \wedge Q \wedge (R \vee \neg R)) \vee (\neg P \wedge R \wedge (Q \vee \neg Q))$

$\vee (Q \wedge R \wedge (P \vee \neg P))$

$\Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge R \wedge Q)$

$\vee (\neg P \wedge R \wedge \neg Q)$

例题 9 试求 $P \to ((P \to Q) \wedge \neg(\neg Q \vee \neg P))$ 的主析取范式。

解 $P\to((P\to Q)\wedge\neg(\neg Q\vee\neg P))$

$$\Leftrightarrow\neg P\vee((\neg P\vee Q)\wedge(Q\wedge P))$$
$$\Leftrightarrow\neg P\vee((\neg P\wedge Q\wedge P)\vee(Q\wedge Q\wedge P))$$
$$\Leftrightarrow\neg P\vee(\neg P\wedge Q\wedge P)\vee(Q\wedge P)$$
$$\Leftrightarrow\neg P\vee(Q\wedge P)$$
$$\Leftrightarrow(\neg P\wedge(Q\vee\neg Q))\vee(Q\wedge P)$$
$$\Leftrightarrow(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(P\wedge Q)$$

由上述各例我们看到，一个命题公式的主析取范式，可由两种方法构成。一是由公式的真值表得出，另一是由基本等价公式推出。其推演步骤可归纳为：

(1) 化归为析取范式。

(2) 除去析取范式中所有永假的析取项。

(3) 将析取式中重复出现的合取项和相同的变元合并。

(4) 对合取项补入没有出现的命题变元，即添加 $(P\wedge\neg P)$ 式，然后，应用分配律展开公式。

对于一个命题公式的主析取范式，如将其命题变元的个数及出现次序固定后，则此公式的主析取范式便是唯一的，因此，给定任两个公式，由主析取范式可以方便地看出两个公式是否等价。

与主析取范式类似的是主合取范式。

定义 1-7.6 n 个命题变元的析取式，称作布尔析取或大项。其中每个变元与它的否定不能同时存在，但两者必须出现且仅出现一次。例如

$$P\vee Q,\ P\vee\neg Q,\ \neg P\vee Q,\ \neg P\vee\neg Q$$

又如 $P\vee Q\vee R,\ P\vee Q\vee\neg R,\ \cdots,\ \neg P\vee\neg Q\vee\neg R$

每个大项可用 n 位二进制予以编码：

若 $n=2$

$M_{00}=P\vee Q,\qquad M_{01}=P\vee\neg Q$

$M_{10}=\neg P\vee Q,\qquad M_{11}=\neg P\vee\neg Q$

若 $n=3$

$M_{000}=P\vee Q\vee R,\qquad M_{100}=\neg P\vee Q\vee R$

$$M_{001}=P\vee Q\vee\neg R,\qquad M_{101}=\neg P\vee Q\vee\neg R$$

$$M_{010}=P\vee\neg Q\vee R,\qquad M_{110}=\neg P\vee\neg Q\vee R$$

$$M_{011}=P\vee\neg Q\vee\neg R,\quad M_{111}=\neg P\vee\neg Q\vee\neg R$$

大项有如下性质:

(1) 每个大项当其真值指派与编码相同时，其真值为 $\boldsymbol{F}$，在其余 2^n-1 种指派情况下均为 $\boldsymbol{T}$。

(2) 任意两个不同大项的析取式为永真。

$$M_i\vee M_j\Leftrightarrow \boldsymbol{T}\quad(i\neq j)$$

(3) 全体大项的合取式必为永假，记为:

$$\prod_{i=0}^{2^n-1}M_i=M_0\wedge M_1\wedge\cdots\wedge M_{2^n-1}\Leftrightarrow \boldsymbol{F}$$

定义 1-7.7 对于给定的命题公式，如果有一个等价公式，它仅由大项的合取所组成，则该等价式称作原式的主合取范式。

一个公式的主合取范式亦可用真值表的方法予以写出。

定理 1-7.4 在真值表中，一个公式的真值为 $\boldsymbol{F}$ 的指派所对应的大项的合取，即为此公式的主合取范式。

证法与定理 1-7.3 相同。 □

例题 10 利用真值表技术求 $(P\wedge Q)\vee(\neg P\wedge R)$ 的主合取范式与主析取范式。

解 公式 $(P\wedge Q)\vee(\neg P\wedge R)$ 的真值表如表 1-7.5 所示。

表 1-7.5

P	Q	R	$P\wedge Q$	$\neg P\wedge R$	$(P\wedge Q)\vee(\neg P\wedge R)$
T	**T**	**T**	**T**	**F**	**T**
T	**T**	**F**	**T**	**F**	**T**
T	**F**	**T**	**F**	**F**	**F**
T	**F**	**F**	**F**	**F**	**F**
F	**T**	**T**	**F**	**T**	**T**
F	**T**	**F**	**F**	**F**	**F**
F	**F**	**T**	**F**	**T**	**T**
F	**F**	**F**	**F**	**F**	**F**

故主合取范式为:

$$(P\wedge Q)\vee(\neg P\wedge R)\Leftrightarrow(\neg P\vee Q\vee\neg R)\wedge(\neg P\vee Q\vee R)\wedge(P\vee\neg Q\vee R)\wedge(P\vee Q\vee R)$$

主析取范式为:

$$(P\wedge Q)\vee(\neg P\wedge R)\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)\vee(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge R)$$

一个公式的主合取范式,亦可用基本等价式推出,其推演步骤为:

(1) 化归为合取范式。

(2) 除去合取范式中所有为永真的合取项。

(3) 合并相同的析取项和相同的变元。

(4) 对析取项补入没有出现的命题变元,即添加 $(P\vee\neg P)$ 式,然后,应用分配律展开公式。

例题 11 化 $(P\wedge Q)\vee(\neg P\wedge R)$ 为主合取范式。

解

$$\begin{aligned}(P\wedge Q)\vee(\neg P\wedge R)&\Leftrightarrow((P\wedge Q)\vee\neg P)\wedge((P\wedge Q)\vee R)\\&\Leftrightarrow(P\vee\neg P)\wedge(Q\vee\neg P)\wedge(P\vee R)\wedge(Q\vee R)\\&\Leftrightarrow(Q\vee\neg P)\wedge(P\vee R)\wedge(Q\vee R)\\&\Leftrightarrow(Q\vee\neg P\vee(R\wedge\neg R))\wedge(P\vee R\vee(Q\wedge\neg Q))\\&\quad\wedge(Q\vee R\vee(P\wedge\neg P))\\&\Leftrightarrow(Q\vee\neg P\vee R)\wedge(Q\vee\neg P\vee\neg R)\wedge(P\vee R\vee Q)\\&\quad\wedge(P\vee R\vee\neg Q)\wedge(Q\vee R\vee P)\wedge(Q\vee R\vee\neg P)\\&\Leftrightarrow(\neg P\vee Q\vee R)\wedge(\neg P\vee Q\vee\neg R)\\&\quad\wedge(P\vee\neg Q\vee R)\wedge(P\vee Q\vee R)\end{aligned}$$

为了使主析取范式和主合取范式表达简洁,我们今后用 Σ 表示小项的析取,$\Sigma i, j, k$,即表示 $m_i\vee m_j\vee m_k$; 用 Π 表示大项的合取,$\Pi i, j, k$ 表示 $M_i\wedge M_j\wedge M_k$,由这样的约定,例题 10 可以表达为:

$$(P\wedge Q)\vee(\neg P\wedge R)\Leftrightarrow m_{001}\vee m_{011}\vee m_{110}\vee m_{111}=\Sigma_{1,3,6,7}$$

$$(P\wedge Q)\vee(\neg P\wedge R)\Leftrightarrow M_{000}\wedge M_{010}\wedge M_{100}\wedge M_{101}=\Pi_{0,2,4,5}$$

可以证明,如果命题公式 P 的主析取范式为:

$$\Sigma i_1,\ i_2,\ \cdots,\ i_k$$

则 P 的主合取范式为：

$\Pi 0, 1, 2, \cdots, i_1-1, i_1+1, \cdots, i_k-1, i_k+1, \cdots, 2^n-1$

1-7 习题

(1) 求公式 $P\wedge(P\to Q)$ 的析取范式和合取范式。

(2) 把下列各式化为析取范式。

a) $(\neg P\wedge Q)\to R$

b) $P\to((Q\wedge R)\to S)$

c) $\neg(P\vee\neg Q)\wedge(S\to T)$

d) $(P\to Q)\to R$

e) $\neg(P\wedge Q)\wedge(P\vee Q)$

(3) 把下列各式化为合取范式。

a) $P\vee(\neg P\wedge Q\wedge R)$

b) $\neg(P\to Q)\vee(P\vee Q)$

c) $\neg(P\to Q)$

d) $(P\to Q)\to R$

e) $(\neg P\wedge Q)\vee(P\wedge\neg Q)$

(4) 求下列各式的主析取范式及主合取范式，并指出下列各式哪些是重言式。

a) $(\neg P\vee\neg Q)\to(P\rightleftarrows\neg Q)$

b) $Q\wedge(P\vee\neg Q)$

c) $P\vee(\neg P\to(Q\vee(\neg Q\to R)))$

d) $(P\to(Q\wedge R))\wedge(\neg P\to(\neg Q\wedge\neg R))$

e) $P\to(P\wedge(Q\to P))$

f) $(Q\to P)\wedge(\neg P\wedge Q)$

(5) 用将合式公式化为范式的方法证明下列各题中两式是等价的。

a) $(A\to B)\wedge(A\to C)$, $A\to(B\wedge C)$

b) $(A\to B)\to(A\wedge B)$, $(\neg A\to B)\wedge(B\to A)$

c) $A\wedge B\wedge(\neg A\vee\neg B)$, $\neg A\wedge\neg B\wedge(A\vee B)$

d) $A\vee(A\to(A\wedge B))$, $\neg A\vee\neg B\vee(A\wedge B)$

(6) 如果 $A(P, Q, R)$ 由 $R\uparrow(Q\wedge\neg(R\downarrow P))$ 给出，求它的对偶 $A^*(P, Q, R)$，并求出与 A 及 A^* 等价且仅包含联结词"$\wedge$"，"$\vee$"及"$\neg$"的公式。

(7) A, B, C, D 四个人中要派两个人出差，按下述三个条件有几种派法？如何派？

① 若 A 去则 C 和 D 中要去一人;

② B 和 C 不能都去;

③ C 去则 D 要留下。

(8) 三人估计比赛结果，甲说"A 第一，B 第二"。乙说"C 第二，D 第四"。丙说"A 第二，D 第四"。结果三人估计得都不全对，但都对了一个，问 A、B、C、D 的名次。

1-8 推理理论

在数学和其它自然科学中，经常要考虑从某些前提 $A_1, A_2, \cdots, A_n$ 能够推导出什么结论。例如从分子学说，原子学说，能够得到什么结论，从光的波动学说，能得到什么结论等等。我们一般地要对"假设"的内容作深入分析，并推究其间的关系，从而得到结论。但也有一些推理，只需分析假设中的真值和联结词，便可获得结论。

在实际应用的推理中，我们常常把本门学科的一些定律、定理和条件，作为假设前提，尽管这些前提在数理逻辑中实非永真，但在推理过程中，却总是假设这些命题为 T，并使用一些公认的规则，得到另外的命题，形成结论，这种过程就是论证。

定义 1-8.1 设 A 和 C 是两个命题公式，当且仅当 $A \to C$ 为一重言式，即 $A \Rightarrow C$，称 C 是 A 的有效结论。或 C 可由 A 逻辑地推出。

这个定义可以推广到有 n 个前提的情况。

设 $H_1, H_2, \cdots, H_n, C$ 是命题公式，当且仅当

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C \qquad \text{(A)}$$

称 C 是一组前提 $H_1, H_2, \cdots, H_n$ 的有效结论。

判别有效结论的过程就是论证过程，论证方法千变万化，但基本方法是真值表法、直接证法和间接证法。

(1) *真值表法*

设 $P_1, P_2, \cdots, P_n$ 是出现于前提 $H_1, H_2, \cdots, H_m$ 和结论 C 中的全部命题变元，假定对 $P_1, P_2, \cdots, P_n$ 作了全部的真值指派，

这样就能对应地确定 $H_1, H_2, \cdots, H_m$ 和 C 的所有真值，列出这个真值表，即可看出(A)式是否成立。

因为若从真值表上找出 $H_1, H_2, \cdots, H_m$ 真值均为 $\boldsymbol{T}$ 的行，对于每一个这样的行，若 C 也有真值 $\boldsymbol{T}$，则(A)式成立，或者看 C 的真值为 $\boldsymbol{F}$ 的行，在每一个这样的行中，$H_1, H_2, \cdots, H_m$ 的真值中至少有一个为 $\boldsymbol{F}$，则(A)式也成立。现举例说明如下。

例题 1 一份统计表格的错误或者是由于材料不可靠，或者是由于计算有错误；这份统计表格的错误不是由于材料不可靠，所以这份统计表格是由于计算有错误。

解 设各命题变元为

P：统计表格的错误是由于材料不可靠。

Q：统计表格的错误是由于计算有错误。

本例可译为：Q 是前提 $P\vee Q$，$\neg P$ 的有效结论，即

$$\neg P\wedge(P\vee Q)\Rightarrow Q$$

我们列出真值表 1-8.1 如下：

表 1-8.1

P	Q	$P\vee Q$	$\neg P$
$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{T}$	$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{T}$	$\boldsymbol{T}$	$\boldsymbol{T}$
$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{F}$	$\boldsymbol{T}$

从表上看到只有在第三行 $P\vee Q$ 和 $\neg P$ 的真值都为 $\boldsymbol{T}$，这时 Q 的真值亦为 $\boldsymbol{T}$。故

$$(P\vee Q)\wedge(\neg P)\Rightarrow Q$$

成立。

或者考察 Q 的真值为 $\boldsymbol{F}$ 的情况，在第二行和第四行，其相应的 $P\vee Q$ 或 $\neg P$ 中至少有一真值为 $\boldsymbol{F}$，故亦说明 $(P\vee Q)\wedge(\neg P)\Rightarrow Q$ 成立。

例题 2 如果张老师来了，这个问题可以得到解答，如果李老师来了，这个问题也可以得到解答，总之张老师或李老师来了，这个问题就可得到解答。

解 若设 P：张老师来了。

Q：李老师来了。

R: 这个问题可以得到解答。

上述语句可翻译成下述命题关系式

$$(P\to R)\wedge(Q\to R)\wedge(P\vee Q)\Rightarrow R$$

列出真值表 1-8.2 如下

表 1-8.2

P	Q	R	$P\to R$	$Q\to R$	$P\vee Q$
T	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**F**	**F**	**T**
T	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**T**	**T**
F	**T**	**T**	**T**	**T**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**F**	**T**	**T**	**T**	**F**
F	**F**	**F**	**T**	**T**	**F**

从真值表看到，$P\to R$, $Q\to R$, $P\vee Q$ 的真值都为 **T** 的情况为第一行、第三行和第五行，而在这三行中 R 的真值均为 **T**。故

$$(P\to R)\wedge(Q\to R)\wedge(P\vee Q)\Rightarrow R$$

(2) *直接证法*

直接证法就是由一组前提，利用一些公认的推理规则，根据已知的等价或蕴含公式，推演得到有效的结论。

P 规则　前提在推导过程中的任何时候都可以引入使用。

T 规则　在推导中，如果有一个或多个公式、重言蕴含着公式 S，则公式 S 可以引入推导之中。

现将常用的蕴含式和等价式列入表 1-8.3 和表 1-8.4 中。

例题 1　证明　$(P\vee Q)\wedge(P\to R)\wedge(Q\to S)\Rightarrow S\vee R$

证法 1
(1) $P\vee Q$　　　P
(2) $\neg P\to Q$　　　T(1) E
(3) $Q\to S$　　　P
(4) $\neg P\to S$　　　T(2),(3) I

表 1-8.3

I_1	$P\wedge Q\Rightarrow P$
I_2	$P\wedge Q\Rightarrow Q$
I_3	$P\Rightarrow P\vee Q$
I_4	$Q\Rightarrow P\vee Q$
I_5	$\neg P\Rightarrow P\rightarrow Q$
I_6	$Q\Rightarrow P\rightarrow Q$
I_7	$\neg(P\rightarrow Q)\Rightarrow P$
I_8	$\neg(P\rightarrow Q)\Rightarrow\neg Q$
I_9	$P, Q\Rightarrow P\wedge Q$
I_{10}	$\neg P,\ P\vee Q\Rightarrow Q$
I_{11}	$P,\ P\rightarrow Q\Rightarrow Q$
I_{12}	$\neg Q,\ P\rightarrow Q\Rightarrow\neg P$
I_{13}	$P\rightarrow Q,\ Q\rightarrow R\Rightarrow P\rightarrow R$
I_{14}	$P\vee Q,\ P\rightarrow R,\ Q\rightarrow R\Rightarrow R$
I_{15}	$A\rightarrow B\Rightarrow(A\vee C)\rightarrow(B\vee C)$
I_{16}	$A\rightarrow B\Rightarrow(A\wedge C)\rightarrow(B\wedge C)$

表 1-8.4

E_1	$\neg\neg P\Leftrightarrow P$
E_2	$P\wedge Q\Leftrightarrow Q\wedge P$
E_3	$P\vee Q\Leftrightarrow Q\vee P$
E_4	$(P\wedge Q)\wedge R\Leftrightarrow P\wedge(Q\wedge R)$
E_5	$(P\vee Q)\vee R\Leftrightarrow P\vee(Q\vee R)$
E_6	$P\wedge(Q\vee R)\Leftrightarrow(P\wedge Q)\vee(P\wedge R)$
E_7	$P\vee(Q\wedge R)\Leftrightarrow(P\vee Q)\wedge(P\vee R)$
E_8	$\neg(P\wedge Q)\Leftrightarrow\neg P\vee\neg Q$
E_9	$\neg(P\vee Q)\Leftrightarrow\neg P\wedge\neg Q$
E_{10}	$P\vee P\Leftrightarrow P$
E_{11}	$P\wedge P\Leftrightarrow P$
E_{12}	$R\vee(P\wedge\neg P)\Leftrightarrow R$
E_{13}	$R\wedge(P\vee\neg P)\Leftrightarrow R$
E_{14}	$R\vee(P\vee\neg P)\Leftrightarrow\mathbf{T}$
E_{15}	$R\wedge(P\wedge\neg P)\Leftrightarrow\mathbf{F}$
E_{16}	$P\rightarrow Q\Leftrightarrow\neg P\vee Q$
E_{17}	$\neg(P\rightarrow Q)\Leftrightarrow P\wedge\neg Q$
E_{18}	$P\rightarrow Q\Leftrightarrow\neg Q\rightarrow\neg P$
E_{19}	$P\rightarrow(Q\rightarrow R)\Leftrightarrow(P\wedge Q)\rightarrow R$
E_{20}	$P\rightleftarrows Q\Leftrightarrow(P\rightarrow Q)\wedge(Q\rightarrow P)$
E_{21}	$P\rightleftarrows Q\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge\neg Q)$
E_{22}	$\neg(P\rightleftarrows Q)\Leftrightarrow P\rightleftarrows\neg Q$

	(5) $\neg S \to P$	$T(4)\ E$
	(6) $P \to R$	P
	(7) $\neg S \to R$	$T(5),(6)\ I$
	(8) $S \vee R$	$T(7)\ E$
证法 2	(1) $P \to R$	P
	(2) $P \vee Q \to R \vee Q$	$T(1)\ I$
	(3) $Q \to S$	P
	(4) $Q \vee R \to S \vee R$	$T(3)\ I$
	(5) $P \vee Q \to S \vee R$	$T(2),(4)\ I$
	(6) $P \vee Q$	P
	(7) $S \vee R$	$T(5),(6)\ I$

例题 3 证明

$$(W \vee R) \to V,\ V \to C \vee S,\ S \to U,\ \neg C \wedge \neg U \Rightarrow \neg W$$

证明	(1) $\neg C \wedge \neg U$	P
	(2) $\neg U$	$T(1)\ I$
	(3) $S \to U$	P
	(4) $\neg S$	$T(2),(3)\ I$
	(5) $\neg C$	$T(1)\ I$
	(6) $\neg C \wedge \neg S$	$T(4),(5)\ I$
	(7) $\neg(C \vee S)$	$T(6)\ E$
	(8) $(W \vee R) \to V$	P
	(9) $V \to (C \vee S)$	P
	(10) $(W \vee R) \to (C \vee S)$	$T(8),(9)\ I$
	(11) $\neg(W \vee R)$	$T(7),(10)\ I$
	(12) $\neg W \wedge \neg R$	$T(11)\ E$
	(13) $\neg W$	$T(12)\ I$

(3) 间接证法

定义 1-8.2 假设公式 $H_1, H_2, \cdots, H_m$ 中的命题变元为 $P_1, P_2, \cdots, P_n$，对于 $P_1, P_2, \cdots, P_n$ 的一些真值指派，如果能使 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 的真值为 $\boldsymbol{T}$，则称公式 $H_1, H_2, \cdots, H_m$ 是相容的。如果对于 $P_1, P_2, \cdots\cdots, P_n$ 的每一组真值指派使得 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 的真值均为 $\boldsymbol{F}$，则称公式 $H_1, H_2, \cdots\cdots, H_m$ 是不相容的。

现在可把不相容的概念应用于命题公式的证明。

设有一组前提 $H_1, H_2, \cdots, H_m$，要推出结论 C，即证 $H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow C$，记作 $S \Rightarrow C$，即 $\neg C \rightarrow \neg S$ 为永真，或 $C \vee \neg S$ 为永真，故 $\neg C \wedge S$ 为永假。因此要证明 $H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow C$，只要证明 $H_1, H_2, \cdots, H_m$ 与 $\neg C$ 是不相容的。

例题 3 证明 $A \rightarrow B$，$\neg(B \vee C)$ 可逻辑推出 $\neg A$

证明(1) $A \rightarrow B$ $\qquad P$

(2) A $\qquad P$(附加前提)

(3) $\neg(B \vee C)$ $\qquad P$

(4) $\neg B \wedge \neg C$ $\qquad T(3)\ E$

(5) B $\qquad T(1),(2)\ I$

(6) $\neg B$ $\qquad T(4)\ I$

(7) $B \wedge \neg B$(矛盾) $\qquad T(5),(6)\ I$

例题 4 证明 $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S) \Rightarrow S \vee R$

证明(1) $\neg(S \vee R)$ $\qquad P$(附加前提)

(2) $\neg S \wedge \neg R$ $\qquad T(1)\ E$

(3) $P \vee Q$ $\qquad P$

(4) $\neg P \rightarrow Q$ $\qquad T(3)\ E$

(5) $Q \rightarrow S$ $\qquad P$

(6) $\neg P \rightarrow S$ $\qquad T(4),(5)\ I$

(7) $\neg S \rightarrow P$ $\qquad T(6)\ E$

(8) $(\neg S \wedge \neg R) \rightarrow (P \wedge \neg R)$ $\qquad T(7)\ I$

(9) $P \wedge \neg R$ $\qquad T(2),(8)\ I$

(10) $P \rightarrow R$ $\qquad P$

(11) $\neg P \vee R$ $\qquad T(10)\ E$

(12) $\neg(P \wedge \neg R)$ $\qquad T(11)\ E$

(13) $(P \wedge \neg R) \wedge \neg(P \wedge \neg R)$(矛盾) $\qquad T(9),(12)\ I$

间接证法的另一种情况是：若要证 $H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow (R \rightarrow C)$。设 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 为 S，即证 $S \Rightarrow (R \rightarrow C)$ 或 $S \Rightarrow (\neg R \vee C)$，故 $S \rightarrow (\neg R \vee C)$ 为永真式。因为 $S \rightarrow (\neg R \vee C) \Leftrightarrow \neg S \vee (\neg R \vee C) \Leftrightarrow (\neg S \vee \neg R) \vee C \Leftrightarrow \neg(S \wedge R) \vee C \Leftrightarrow (S \wedge R) \rightarrow C$，所以若将 R 作附加前提，如有 $(S \wedge R) \Rightarrow C$，即证得 $S \Rightarrow (R \rightarrow C)$。由 $(S \wedge R) \Rightarrow C$，证得 $S \Rightarrow (R \rightarrow C)$ 称为 CP 规则。

例题 5 证明 $A \to (B \to C)$, $\neg D \vee A$, B 重言蕴含 $D \to C$

证明(1) D　　P(附加前提)

(2) $\neg D \vee A$　　P

(3) A　　T(1), (2) I

(4) $A \to (B \to C)$　　P

(5) $B \to C$　　T(3), (4) I

(6) B　　P

(7) C　　T(5), (6) I

(8) $D \to C$　　CP

例题 6 设有下列情况,结论是否有效?

(a) 或者是天晴,或者是下雨。

(b) 如果是天晴,我去看电影。

(c) 如果我去看电影,我就不看书。

结论: 如果我在看书则天在下雨。

解 若设 M: 天晴。　　Q: 下雨。

S: 我看电影。　　R: 我看书。

故本题即证: $M \overline{\vee} Q$, $M \to S$, $S \to \neg R$, 推出 $R \to Q$

因为 $(M \overline{\vee} Q) \Leftrightarrow \neg(M \rightleftarrows Q)$

(1) R　　P(附加前提)

(2) $S \to \neg R$　　P

(3) $B \to \neg S$　　T(2) E

(4) $\neg S$　　T(1) (3) I

(5) $M \to S$　　P

(6) $\neg M$　　T(4), (5) I

(7) $\neg(M \rightleftarrows Q)$　　P

(8) $M \rightleftarrows \neg Q$　　T(7) E

(9) $(M \to \neg Q) \wedge (\neg Q \to M)$　　T(8) E

(10) $\neg Q \to M$　　T(9) I

(11) $\neg M \to Q$　　T(10) E

(12) Q　　T(6), (11) I

(13) $R \to Q$　　CP

1-8 习题

(1) 用推理规则证明以下各式。

a) $\neg(P \wedge \neg Q)$, $\neg Q \vee R$, $\neg R \Rightarrow \neg P$

b) $J \rightarrow (M \vee N), (H \vee G) \rightarrow J, H \vee G \Rightarrow M \vee N$

c) $B \wedge C, (B \rightleftarrows C) \rightarrow (H \vee G) \Rightarrow G \vee H$

d) $P \rightarrow Q, (\neg Q \vee R) \wedge \neg R, \neg(\neg P \wedge S) \Rightarrow \neg S$

(2) 仅用规则 P 和 T，推证以下公式。

a) $\neg A \vee B, C \rightarrow \neg B \Rightarrow A \rightarrow \neg C$

b) $A \rightarrow (B \rightarrow C), (C \wedge D) \rightarrow E, \neg F \rightarrow (D \wedge \neg E) \Rightarrow A \rightarrow (B \rightarrow F)$

c) $A \vee B \rightarrow C \wedge D, D \vee E \rightarrow F \Rightarrow A \rightarrow F$

d) $A \rightarrow (B \wedge C), \neg B \vee D, (E \rightarrow \neg F) \rightarrow \neg D, B \rightarrow (A \wedge \neg E) \Rightarrow B \rightarrow E$

e) $(A \rightarrow B) \wedge (C \rightarrow D), (B \rightarrow E) \wedge (D \rightarrow F), \neg(E \wedge F), A \rightarrow C \Rightarrow \neg A$

(3) 用 CP 规则推证上题中的 a), b), c), d)各式。

(4) 证明下列各式。(如果必要，可用间接证法。)

a) $(R \rightarrow \neg Q), R \vee S, S \rightarrow \neg Q, P \rightarrow Q \Rightarrow \neg P$

b) $S \rightarrow \neg Q, S \vee R, \neg R, \neg R \rightleftarrows Q \Rightarrow \neg P$

c) $\neg(P \rightarrow Q) \rightarrow \neg(R \vee S), ((Q \rightarrow P) \vee \neg R), R \Rightarrow P \rightleftarrows Q$

(5) 对下面的每一组前提，写出可能导出的结论以及所应用的推理规则。

a) 如果我跑步，那么，我很疲劳。
   我没有疲劳。

b) 如果他犯了错误，那么，他神色慌张。
   他神色慌张。

c) 如果我的程序通过，那么，我很快乐。
   如果我快乐，那么，阳光很好。
   现在是晚上十一点，天很暖。

*1-9 应　　用

我们可以将学过的命题逻辑知识应用于日常生活和工程技术中，特别是在电路设计中应用更广。为了今后组合电路逻辑设计的需要，现将与命题逻辑联结词相对应的门电路汇总于图 1-9.1。

下面给出一些综合应用例题。

例题 1 一家航空公司，为了保证安全，用计算机复核飞行计划。每台计算机能给出飞行计划正确或有误的回答。由于计算机也可能发生故障，因此采用三台计算机同时复核。由所给答案，再根据"少数服从多数"的原则作出判断，试将结果用命题公式表示，并加以简化，画出电路图。

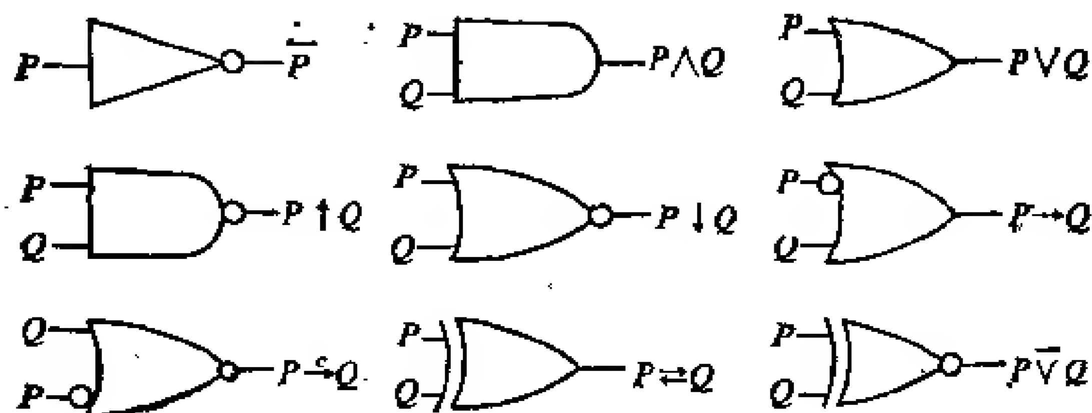


图 1-9.1

解：设 C_1, C_2, C_3 分别表示三台计算机的答案。S 表示判断结果。根据题意有 1-9.1 表的真值表。

表 1-9.1

C_1	C_2	C_3	S
F	F	F	F
F	F	T	F
F	T	F	F
F	T	T	T
T	F	F	F
T	F	T	T
T	T	F	T
T	T	T	T

$$
\begin{aligned}
S &\Leftrightarrow (\neg C_1 \wedge C_2 \wedge C_3) \vee (C_1 \wedge \neg C_2 \wedge C_3) \\
&\quad \vee (C_1 \wedge C_2 \wedge \neg C_3) \vee (C_1 \wedge C_2 \wedge C_3) \\
&\Leftrightarrow ((\neg C_1 \vee C_1) \wedge C_2 \wedge C_3) \vee (C_1 \wedge (\neg C_2 \vee C_2) \wedge C_3) \\
&\quad \vee (C_1 \wedge C_2 \wedge (C_3 \vee \neg C_3)) \\
&\Leftrightarrow (C_2 \wedge C_3) \vee (C_1 \wedge C_3) \vee (C_1 \wedge C_2)
\end{aligned}
$$

电路图如图 1-9.2 所示。

例题 2 有一会议室，四周都有出入门，门旁装有开关（双态开关）。为了控制全室的照明，要求设计一个线路，使得改变任一只开关的状态，就能改

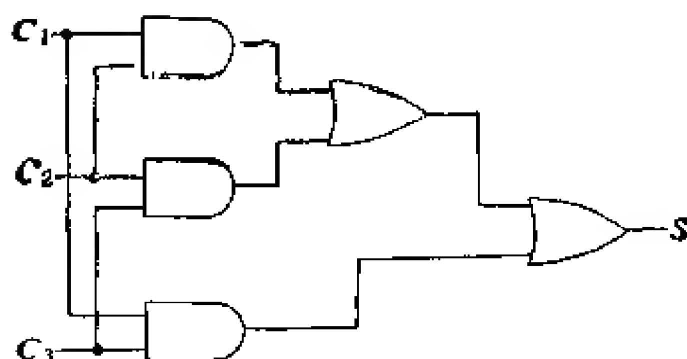


图 1-9.2

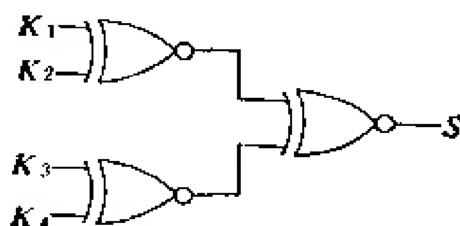


图 1-9.3

变全室的明暗。假设，室中无人时灯暗，有人时灯亮。写出控制电路的逻辑表达式并画出电路图。

解　会议室四扇门旁的开关表示为 K_1, K_2, K_3, K_4。"0" 表示开关断开，"1" 表示开关接通。S 表示会议室的照明状态，"1" 表示全室灯亮，"0" 表示全室灯暗。

假设开始时，室内无人，灯暗，四只开关都处于 "0" 状态。有人进入室内时，随手改变门旁的开关状态，则会议室灯亮，S 为 "1"。此时四只开关中有三只(奇数)处于 "0" 状态。最后一个人离开会议室时，随手改变门旁的开关状态，会议室灯暗，S 为 "0"。如果该门恰是首次进入的门，则四只(偶数)开关都处于"0"状态。如果该门是另一扇门，则有两只(偶数)处于 "0" 状态。以此类推，总之，当有偶数只开关处于 "0" 状态时，S 为 "0"。有奇数只开关处于 "0" 状态，则 S 为 "1"，所以，我们有：

$$
\begin{aligned}
S \Leftrightarrow & (\neg K_1 \wedge \neg K_2 \wedge \neg K_3 \wedge K_4) \vee (\neg K_1 \wedge \neg K_2 \wedge K_3 \wedge \neg K_4) \\
& \vee (\neg K_1 \wedge K_2 \wedge \neg K_3 \wedge \neg K_4) \vee (K_1 \wedge \neg K_2 \wedge \neg K_3 \wedge \neg K_4) \\
& \vee (\neg K_1 \wedge K_2 \wedge K_3 \wedge K_4) \vee (K_1 \wedge \neg K_2 \wedge K_3 \wedge K_4) \\
& \vee (K_1 \wedge K_2 \wedge \neg K_3 \wedge K_4) \vee (K_1 \wedge K_2 \wedge K_3 \wedge \neg K_4) \\
\Leftrightarrow & (\neg K_1 \wedge \neg K_2 \wedge (K_3 \overline{\vee} K_4)) \vee (\neg K_3 \wedge \neg K_4 \wedge (K_1 \overline{\vee} K_2)) \\
& \vee (K_3 \wedge K_4 \wedge (K_1 \overline{\vee} K_2)) \vee (K_1 \wedge K_2 \wedge (K_3 \overline{\vee} K_4)) \\
\Leftrightarrow & (\neg (K_1 \overline{\vee} K_2) \wedge (K_3 \overline{\vee} K_4)) \vee ((K_1 \overline{\vee} K_2) \wedge \neg (K_3 \overline{\vee} K_4)) \\
\Leftrightarrow & (K_1 \overline{\vee} K_2) \overline{\vee} (K_3 \overline{\vee} K_4)
\end{aligned}
$$

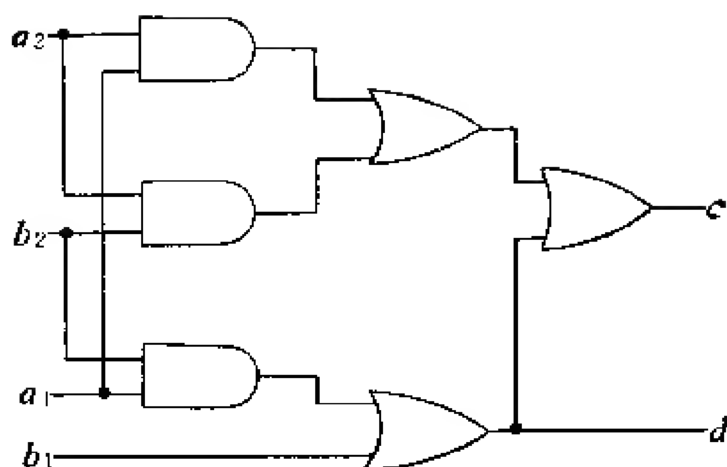


图 1-9.4

电路图如图 1-9.3 所示。

例题 3 设计一台自动售货机，它只能接受一分和二分硬币，当投入硬币总值超过三分时，给出一根棒糖，并找回余额。

解 将投入硬币的情况分别表示为：

$A=[a_1, a_2]$

[0, 0]	投入 0 个一分硬币
[0, 1]	投入 1 个一分硬币
[1, 0]	投入 2 个一分硬币
[1, 1]	投入 3 个一分硬币

$B=[b_1, b_2]$

[0, 0]	投入 0 个二分硬币
[0, 1]	投入 1 个二分硬币
[1, 0]	投入 2 个二分硬币
[1, 1]	投入 3 个二分硬币

$C=[c]$

[0]	投入硬币总额不满三分，不给棒糖
[1]	投入硬币总额超过三分，给出一根棒糖

$D=[d]$

[0]	无余额找
[1]	要找余额

根据题意，有真值表 1-9.2。

$$c \Leftrightarrow (\neg a_1 \wedge \neg a_2 \wedge b_1 \wedge \neg b_2) \vee (\neg a_1 \wedge \neg a_2 \wedge b_1 \wedge b_2)$$
$$\vee (\neg a_1 \wedge a_2 \wedge \neg b_1 \wedge b_2) \vee (\neg a_1 \wedge a_2 \wedge b_1 \wedge \neg b_2)$$

表 1-9.2

a_1	a_2	b_1	b_2	c	d
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	1	1
0	0	1	1	1	1
0	1	0	0	0	0
0	1	0	1	1	0
0	1	1	0	1	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	1	1	1
1	0	1	0	1	1
1	0	1	1	1	1
1	1	0	0	1	0
1	1	0	1	1	1
1	1	1	0	1	1
1	1	1	1	1	1

$$\vee(\neg a_1\wedge a_2\wedge b_1\wedge b_2)\vee(a_1\wedge\neg a_2\wedge\neg b_1\wedge b_2)$$
$$\vee(a_1\wedge\neg a_2\wedge b_1\wedge\neg b_2)\vee(a_1\wedge\neg a_2\wedge b_1\wedge b_2)$$
$$\vee(a_1\wedge a_2\wedge\neg b_1\wedge\neg b_2)\vee(a_1\wedge a_2\wedge\neg b_1\wedge b_2)$$
$$\vee(a_1\wedge a_2\wedge b_1\wedge\neg b_2)\vee(a_1\wedge a_2\wedge b_1\wedge b_2)$$
$$\Leftrightarrow(a_1\wedge a_2)\vee(a_2\wedge b_2)\vee(a_1\wedge b_2)\vee b_1$$

$$d\Leftrightarrow(\neg a_1\wedge\neg a_2\wedge b_1\wedge\neg b_2)\vee(\neg a_1\wedge\neg a_2\wedge b_1\wedge b_2)$$
$$\vee(\neg a_1\wedge a_2\wedge b_1\wedge\neg b_2)\vee(\neg a_1\wedge a_2\wedge b_1\wedge b_2)$$
$$\vee(a_1\wedge\neg a_2\wedge\neg b_1\wedge b_2)\vee(a_1\wedge\neg a_2\wedge b_1\wedge\neg b_2)$$
$$\vee(a_1\wedge\neg a_2\wedge b_1\wedge b_2)\vee(a_1\wedge a_2\wedge\neg b_1\wedge b_2)$$
$$\vee(a_1\wedge a_2\wedge b_1\wedge\neg b_2)\vee(a_1\wedge a_2\wedge b_1\wedge b_2)$$
$$\Leftrightarrow(a_1\wedge b_2)\vee b_1$$

对应的电路图如图 1-9.4 所示。

例题 4 有一逻辑学家误入某部落，被拘于牢狱，酋长意欲放行，他对逻辑学家说："今有两门，一为自由，一为死亡，你可任意开启一门。为协助你脱逃，今加派两名战士负责解答你所提的任何问题。惟可虑者，此两战士中一名天性诚实，一名说谎成性，今后生死由你自己选择。"逻辑学家沉思片刻，即向一战士发问，然后开门从容离去。该逻辑学家应如何发问？

解 逻辑学家手指一门问身旁一名战士说："这扇门是死亡门，他（指另一名战士）将回答'是'，对吗？"

当被问战士回答"对"，则逻辑学家开启所指的门从容离去。当被问战士回答"否"，则逻辑学家开启另一门从容离去。

分析：如果被问者是诚实战士，他回答"对"。则另一名战士是说谎战士，他回答"是"，那么，这扇门不是死亡门。

如果被问者是诚实战士，他回答"否"。则另一名是说谎战士，他回答"不是"，那么，这扇门是死亡门。

如果被问者是说谎战士，可以类似分析。

设 P：被问战士是诚实人。

Q：被问战士的回答是"是"。

R：另一战士的回答是"是"。

S：这扇门是死亡门。

我们有真值表 1-9.3。

表 1-9.3

P	Q	R	S
T	T	T	F
T	F	F	T
F	T	F	F
F	F	T	T

$$R \Leftrightarrow P \rightleftarrows Q$$

$$S \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$$

$$\Leftrightarrow (P \vee \neg P) \wedge \neg Q \Leftrightarrow \neg Q$$

因此，当被问人回答"是"时，此门不是死亡门，逻辑学家可开此门从容离去。当被问人回答"否"时，此门是死亡门，逻辑学家可另开一扇门从容离去。

1-9 习题

(1) 银行的金库装有自动报警装置。仅当总经理室的一个人工控制开

关合上时，它才能动作。如果这个人工开关合上，那么当金库的门被撬或者当工作人员尚未切断监视器电源且通向金库的通道上有人时，就要发出警报。试设计这个控制线路。

(2) 设计一个控制盥洗室照明的电路，使得分别装在卧室和盥洗室的两只开关都能控制照明。

(3) 设计一个二进制半加器的电路，它的功能如表1-9.4所示。其中 x 和 y 是被加数，S 是和，C 是进位。

表 1-9.4

x	y	S	C
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

(4) 设计红绿灯自动控制线路。要求传感器中计数器内容 Z，当 $Z \geqslant 5$ 时，亮绿灯，当 $Z \leqslant 2$ 时，亮红灯，当 $2 < Z < 5$ 时，亮黄灯。

第二章 谓词逻辑

在命题逻辑中，主要研究命题和命题演算，其基本组成单位是原子命题，并把它看作不可再分解的。

但是原子命题，实际上还是可以作进一步分析的，特别是两个原子命题间，常常有一些共同特征，为了刻划命题内部的逻辑结构，就需要研究谓词逻辑。

此外，命题逻辑的推证中有着很大的局限性，有些简单的论断也不能用命题逻辑进行推证。

例如，所有的人都是要死的，苏格拉底是人，所以苏格拉底是要死的。

这个简单而有名的苏格拉底三段论，都无法用命题逻辑予以推证。这些都使我们要对命题的内部关系进行深入地研究。

2-1 谓词的概念与表示

命题是反映判断的句子，不反映判断的句子不是命题。一般地说，反映判断的句子是由主语和谓语两部份组成。例如，电子计算机是科学技术的工具。其中"电子计算机"是主语，"是科学技术的工具"是谓语。主语一般是客体，客体可以独立存在，它可以是具体的，也可以是抽象的。例如：小王、老师、3、4、××代表团、唯物主义等。用以刻划客体的性质或关系的即是谓词。例如：张三是个大学生，李四是个大学生，这两个命题可能用不同的符号 P、Q 表示，但是 P 和 Q 的谓语有同样的属性："是个大学生"。因此引入一个符号表示"是个大学生"，再引入一种方法表示客体的名称，这样就能把"××是个大学生"这个命题的本质属性刻划出来。又例如：

(a) 他是三好学生。

(b) 7 是质数。

(c) 每天早晨做广播操是好习惯。

(d) 5 大于 3。

(e) 哥白尼指出地球绕着太阳转。

在上述语句中"是三好学生"、"是质数"、"是好习惯"、"大于"、"指出"都是谓词。前三个是指明客体性质的谓词，后两个是指明两个客体之间关系的谓词。

我们将用大写字母表示谓词，用小写字母表示客体名称，例如 A 表示"是个大学生"，c 表示张三，e 表示李四，则 $A(c)$，$A(e)$ 分别表示"张三是个大学生"，"李四是个大学生"。

用谓词表达命题，必须包括客体和谓词字母两个部份，一般地说，"b 是 A" 类型的命题可用 $A(b)$ 表达。对于 "a 是小于 b" 这种两个客体之间关系的命题，可表达为 $B(a, b)$，这里 B 表示"是小于"。又如命题"点 a 在 b 与 c 之中"可以表示为 L: …在…和…之中，故可记为 $L(a, b, c)$。

我们把 $A(b)$ 称作一元谓词，$B(a, b)$ 称作二元谓词，$L(a, b, c)$ 称作三元谓词，依次类推。

注意，代表客体名称的字母，它在多元谓词表示式中出现的次序与事先约定有关，因此未经约定前，上例记作 $L(a, b, c)$ 或 $L(b c, a)$ 等都可以，但一经约定，$L(a, b, c)$ 与 $L(b, c, a)$ 就代表两个不同的命题。

单独一个谓词不是完整的命题，我们把谓词字母后填以客体所得的式子称为谓词填式，这样谓词和谓词填式应该是两个不同的概念。

一般地说，n 元谓词需要 n 个客体名称插入到固定的位置上，如果 A 为 n 元谓词，$a_1, a_2, \cdots, a_n$ 是客体的名称，则 $A(a_1, a_2, \cdots, a_n)$ 就可成为一个命题。

通常，一元谓词表达了客体的"性质"，而多元谓词表达了客体之间的"关系"。

2-2 命题函数与量词

为了说明命题函数的概念，下面先举例解释命题与谓词的关系。

设 H 是谓词"能够到达山顶"，l 表示客体名称李四，t 表示老虎，c 表示汽车，那么 $H(l)$，$H(t)$，$H(c)$ 等分别表示各个不同的命题，但它们有一个共同的形式，即 $H(x)$。当 x 分别取 l、t、c 时就表示"李四能够到达山顶"，"老虎能够到达山顶"，"汽车能够到达山顶"。

同理，若 $L(x, y)$ 表示"x 小于 y"，那么 $L(2, 3)$ 表示了一个真命题："2 小于 3"。而 $L(5, 1)$ 表示假命题："5 小于 1"。

又如 $A(x, y, z)$ 表示一个关系"x 加上 y 等于 z"。则 $A(3, 2, 5)$ 表示了真命题"$3+2=5$"，而 $A(1, 2, 4)$ 表示了一个假命题"$1+2=4$"。

从上述三个例子中可以看到 $H(x)$，$L(x, y)$，$A(x, y, z)$ 本身不是一个命题，只有当变元 x, y, z 等取特定的客体时，才确定了一个命题。

定义 2-2.1 由一个谓词，一些客体变元组成的表达式称为简单命题函数。

根据这个定义可以看到，n 元谓词就是有 n 个客体变元的命题函数，当 $n=0$ 时，称为 0 元谓词，它本身就是一个命题，故命题是 n 元谓词的一个特殊情况。

由一个或 n 个简单命题函数以及逻辑联结词组合而成的表达式称复合命题函数。

逻辑联结词 $\neg$、$\wedge$、$\vee$、$\rightarrow$、$\rightleftarrows$ 的意义与命题演算中的解释完全类同。

例 1 设 $S(x)$ 表示"x 学习很好"，用 $W(x)$ 表示"x 工作很好"。则 $\neg S(x)$ 表示"x 学习不是很好"。$S(x) \wedge W(x)$ 表示"x 的工作，学习都很好"。$S(x) \rightarrow W(x)$ 表示"若 x 的学习很好，则 x 工作

得很好。”

例 2 用 $H(x, y)$表示“x 比 y 长得高”。设 l 表示李四，c 表示张三。

则 $\neg H(l, c)$ 表示“李四不比张三长得高”。$\neg H(l, c) \wedge \neg H(c, l)$ 表示“李四不比张三长得高”且“张三不比李四长得高”即“张三与李四同样高”。

例 3 设 $Q(x, y)$ 表示“x 比 y 重”，当 x，y 指人或物时，它是一个命题，但若 x，y 指实数时，$Q(x, y)$ 就不是一个命题。

命题函数不是一个命题，只有客体变元取特定名称时，才能成为一个命题。但是客体变元在哪些范围内取特定的值，对是否成为命题及命题的真值极有影响。

例 4 $R(x)$表示“x 是大学生”，如果 x 的讨论范围为某大学里班级中的学生，则 $R(x)$是永真式。

如果 x 的讨论范围为某中学里班级中的学生，则 $R(x)$是永假式。

如果 x 的讨论范围为一个剧场中的观众，观众中有大学生也有非大学生，那么，对某些观众，$R(x)$为真，对另一些观众，$R(x)$为假。

例 5 $(P(x, y) \wedge P(y, z)) \rightarrow P(x, z)$

若 $P(x, y)$解释为“x 小于 y”，当 x,y,z 都在实数域中取值，则这个式子表示为：“若 x 小于 y 且 y 小于 z，则 x 小于 z”。这是一个永真式。

如果 $P(x, y)$解释为“x 为 y 的儿于”，当 x,y,z 都指人，则“若 x 为 y 的儿于且 y 是 z 的儿子则 x 是 z 的儿子”。这个式子表达的是一个永假公式。

如果 $P(x, y)$解释为“x 距离 y 10 米”，若 x，y，z 表示地面上的房子，那么“x 距离 y 10 米且 y 距离 z 10 米则 x 距离 z 10 米”。这个命题的真值将由 x，y，z 的具体位置而定，它可能为 $\boldsymbol{T}$，也可能为 $\boldsymbol{F}$。

从上述两例可以看到，命题函数确定为命题，与客体变元的论述范围有关。在命题函数中，命题变元的论述范围称作个体域。个体域可以是有限的，也可以是无限的，把各种个体域综合在一起作为论述范围的域称全总个体域。

使用上面所讲的一些概念，还不能用符号很好地表达日常生活中的各种命题。例如：$S(x)$表示x是大学生，而x的个体域为某单位的职工。那么$S(x)$可以表示某单位职工都是大学生，也可以表示某单位存在一些职工是大学生。为了避免这种理解上的混乱，因此需要引入量词，以刻划“所有的”和“存在一些”的不同概念。

例如　(a) 所有的人都是要呼吸的。

　　　(b) 每个学生都要参加考试。

　　　(c) 任何整数或是正的或是负的。

这三个例子都需要表示“对所有的x”这样的概念，为此，引入符号$(\forall x)$或(x)，表示“对所有的x”。

若设 $M(x)$：x是人，　$H(x)$：x要呼吸。

　　$P(x)$：x是学生，　$Q(x)$：x要参加考试。

　　$I(x)$：x是整数，　$R(x)$：x是正数，$N(x)$：x是负数。

则上述三例就记为：

(a) $(\forall x)(M(x)\rightarrow H(x))$

(b) $(\forall x)(P(x)\rightarrow Q(x))$

(c) $(\forall x)(I(x)\rightarrow(R(x)\vee N(x)))$

符号“$\forall$”称为全称量词，用来表达“对所有的”“每一个”“对任一个”等。

另外还有一类量词记作$(\exists x)$，表示“存在一些x”。

例如　(a) 存在一个数是质数。

　　　(b) 一些人是聪明的。

　　　(c) 有些人早饭吃面包。

设　$P(x)$：x是质数。

　　$M(x)$：x是人。

$R(x)$：x 是聪明的。

$E(x)$：x 早饭吃面包。

则上述三例可表示为：

(a) $(\exists x)(P(x))$

(b) $(\exists x)(M(x)\wedge R(x))$

(c) $(\exists x)(M(x)\wedge E(x))$

符号"$\exists$"称为存在量词，可用来表达"存在一些""至少有一个""对于一些"等。

全称量词与存在量词统称为量词，在上述有关量词的例子中可以看出，每个由量词确定的表达式，都与个体域有关。例如：$(\forall x)(M(x)\rightarrow H(x))$表示所有的人都要呼吸，如果把个体域限制在"人类"这个范围内，那么亦可简单地表示为$(\forall x)(H(x))$。在这个例子中指定论域，不仅与表达形式有关，而且不同的指定论域会有不同的问题真值。如设论域为"人类"则这个命题的真值为 $\boldsymbol{T}$，如果论域为自然数，则命题的真值为 $\boldsymbol{F}$。为此，在讨论带有量词的命题函数时，必须确定其个体域。为了方便，我们将所有命题函数的个体域全部统一，使用全总个体域。用了这个全总个体域后，对每一个客体变元的变化范围，用特性谓词加以限制。一般地，对全称量词，此特性谓词常作蕴含的前件，对存在量词，此特性谓词常作合取项。例如：在全总个体域中 $(\forall x)(H(x))$ 可写成 $(\forall x)(M(x)\rightarrow H(x))$，其中 $M(x)$为 $H(x)$ 的特性谓词。对$(\exists x)(H(x))$ 可写成$(\exists x)(M(x)\wedge H(x))$，特性谓词 $M(x)$ 限定了 $H(x)$中变元的范围。

2-1, 2-2 习题

(1) 用谓词表达式写出下列命题。

a) 小张不是工人。

b) 他是田径或球类运动员。

c) 小莉是非常聪明和美丽的。

d) 若 m 是奇数，则 $2m$ 不是奇数。

e) 每一个有理数是实数。

f) 某些实数是有理数。

g) 并非每一个实数都是有理数。

h) 直线 A 平行于直线 B，当且仅当直线 A 不相交于直线 B。

(2) 找出以下十二个句子所对应的谓词表达式。

a) 所有教练员是运动员。($J(x)$, $L(x)$)

b) 某些运动员是大学生。($S(x)$)

c) 某些教练是年老的，但是健壮的。($O(x)$, $V(x)$)

d) 金教练既不老但也不是健壮的。(j)

e) 不是所有运动员都是教练。

f) 某些大学生运动员是国家选手。($C(x)$)

g) 没有一个国家选手不是健壮的。

h) 所有老的国家选手都是运动员。

i) 没有一位女同志既是国家选手又是家庭妇女。($W(x)$, $H(x)$)

j) 有些女同志既是教练员又是国家选手。

k) 所有运动员都钦佩某些教练。($A(x, y)$)

l) 有些大学生不钦佩运动员。

2-3 谓词公式与翻译

我们知道，简单命题函数与逻辑联结词可以组合成一些谓词表达式。有了谓词与量词的概念，谓词表达式所能刻划的日常命题就能广泛而深入得多了。但是，怎样的谓词表达式才能成为谓词公式并能进行谓词演算呢？下面先介绍谓词的合式公式。

我们把 $A(x_1, x_2, \cdots, x_n)$ 称作谓词演算的原子公式，其中 $x_1, x_2, \cdots, x_n$ 是客体变元，因此原子谓词公式包括下述形式的各种特例。如：Q, $A(x)$, $A(x, y)$, $A(f(x), y)$, $A(x, y, z)$, $A(a, y)$ 等。

定义 2-3.1 谓词演算的合式公式，[注]可由下述各条组成：

(1) 原子谓词公式是合式公式。

(2) 若 A 是合式公式，则 $\neg A$ 是一个合式公式。

[注] 谓词演算的合式公式的严格定义见"Mathematical Theory of Computation" ZOHAR MANNA. p. 82。

(3) 若 A 和 B 都是合式公式，则 $(A \wedge B)$，$(A \vee B)$，$(A \rightarrow B)$ 和 $(A \rightleftarrows B)$ 是合式公式。

(4) 如果 A 是合式公式，x 是 A 中出现的任何变元，则 $(\forall x)A$ 和 $(\exists x)A$ 都是合式公式。

(5) 只有经过有限次地应用规则 (1)、(2)、(3)、(4) 所得到的公式是合式公式。

在讨论命题公式时，曾用了关于圆括号的某些约定，即最外层的括号可以省略，在谓词合式公式中亦将遵守同样的约定，但需注意，量词后面若有括号则不能省略。

谓词合式公式，今后简称谓词公式。

下面举例说明如何用谓词公式表达自然语言中一些有关命题。

例题 1 并非每个实数都是有理数。$(R(x), Q(x))$

解 $\neg(\forall x)(R(x) \rightarrow Q(x))$

例题 2 没有不犯错误的人。$(F(x), M(x))$

解 $\neg(\exists x(M(x) \wedge \neg F(x)))$

例题 3 尽管有人聪明，但未必一切人都聪明。$(P(x), M(x))$

解 $\exists x(M(x) \wedge P(x)) \wedge \neg(\forall x(M(x) \rightarrow P(x)))$。

例题 4 这只大红书柜摆满了那些古书。

解法 1 设 $F(x, y)$：x 摆满了 y

$R(x)$：　x 是大红书柜

$Q(y)$：　y 是古书

a：这只　b：那些

$$R(a) \wedge Q(b) \wedge F(a, b)$$

解法 2 设 $A(x)$：x 是书柜

$B(x)$：x 是大的

$C(x)$：x 是红的

$D(y)$：y 是古老的

$E(y)$：y 是图书

$F(x, y)$：x 摆满了 y

a：这只　b：那些

$$A(a) \wedge B(a) \wedge C(a) \wedge D(b) \wedge E(b) \wedge F(a, b)$$

由本例可知，对于命题翻译成谓词演算公式，机动性很大，由于对个体描述性质的刻划深度不同，就可翻译成不同形式的谓词公式。本例中 $R(x)$ 表示 x 是大红书柜，而 $A(x)\wedge B(x)\wedge C(x)$ 也可表示大红书柜，但后一种将更方便于对书柜的大小颜色进行讨论，这样对个体刻划深度的不同就可翻译成不同的谓词公式。

例题5 在数学分析中极限定义为：任给小正数 ε，则存在一个正数 δ，使得当 $0<|x-a|<\delta$ 时有 $|f(x)-b|<\varepsilon$。此时即称 $\lim\limits_{x\to a}f(x)=b$。

解 $P(x, y)$ 表示"x 大于 y"，$Q(x, y)$ 表示"x 小于 y"，故 $\lim\limits_{x\to a}f(x)=b$ 可表示为：

$$(\forall\varepsilon)(\exists\delta)(\forall x)(((P(\varepsilon, 0)\to P(\delta, 0))\wedge Q(|x-a|, \delta)\wedge P(|x-a|, 0))\to Q(|f(x)-b|, \varepsilon))$$

2-3 习题

(1) 令 $P(x)$为"x 是质数"； $E(x)$为"x 是偶数"；$O(x)$为"x 是奇数"；$D(x, y)$为"x 除尽 y"。

把以下各式译成汉语：

a) $P(5)$

b) $E(2)\wedge P(2)$

c) $(\forall x)(D(2, x)\to E(x))$

d) $(\exists x)(E(x)\wedge D(x, 6))$

e) $(\forall x)(\neg E(x)\to\neg D(2, x))$

f) $(\forall x)(E(x)\to(\forall y)(D(x, y)\to E(y)))$

g) $(\forall x)(P(x)\to(\exists y)(E(y)\wedge D(x, y)))$

h) $(\forall x)(O(x)\to(\forall y)(P(y)\to\neg D(x, y)))$

(2) 令 $P(x)$, $L(x)$, $R(x, y, z)$和 $E(x, y)$ 分别表示"x 是一个点"，"x 是一条直线"，"z 通过 x 和 y"和"$x=y$"。符号化下面的句子。

对每两个点有且仅有一条直线通过该两点。

(3) 利用谓词公式翻译下列命题。

a) 如果有限个数的乘积为零，那么至少有一个因子等于零。

b) 对于每一个实数 x，存在一个更大的实数 y。

c) 存在实数 x, y 和 z，使得 x 与 y 之和大于 x 与 z 之积。

(4) 用谓词公式写出下式。

若 $x<y$ 和 $z<0$，则 $xz>yz$。

(5) 自然数一共有三条公理。

a) 每个数都有唯一的一个数是它的后继数。

b) 没有一个数使数 1 是它的后继数。

c) 每个不等于 1 的数都有唯一的一个数是它的直接先行者。

用两个谓词表达上述三条公理。

(6) 用谓词公式刻划下述命题。

那位戴眼镜的用功的大学生在看这本大而厚的巨著。

(7) 取个体域为实数集 R, 函数 f 在 a 点连续的定义是: f 在点 a 连续, 当且仅当对每个 $\varepsilon>0$, 存在一个 $\delta>0$, 使得对所有 x, 若 $|x-a|<\delta$, 则 $|f(x)-f(a)|<\varepsilon$。把上述定义用符号化的形式表达。

2-4 变元的约束

给定 α 为一个谓词公式, 其中有一部份公式形式为 $(\forall x)P(x)$ 或 $(\exists x)P(x)$。这里 $\forall$、$\exists$ 后面所跟的 x 叫做量词的指导变元或作用变元, $P(x)$ 叫做相应量词的作用域或辖域。在作用域中 x 的一切出现, 称为 x 在 α 中的约束出现, x 亦称为被相应量词中的指导变元所约束。在 α 中除去约束变元以外所出现的变元称作自由变元。自由变元是不受约束的变元, 虽然它有时也在量词的作用域中出现, 但它不受相应量词中指导变元的约束, 故我们可把自由变元看作是公式中的参数。

例题 1 说明以下各式的作用域与变元约束的情况。

a) $(\forall x)(P(x)\rightarrow Q(x))$

b) $(\forall x)(P(x)\rightarrow(\exists y)R(x, y))$

c) $(\forall x)(\forall y)(P(x, y)\wedge Q(y, z))\wedge(\exists x)P(x, y)$

d) $(\forall x)(P(x)\wedge(\exists x)Q(x, z)\rightarrow(\exists y)R(x, y))\vee Q(x, y)$

解 a) $(\forall x)$ 的作用域是 $P(x)\rightarrow Q(x)$, x 为约束变元。

b) $(\forall x)$ 的作用域是 $(P(x)\rightarrow(\exists y)R(x, y))$, $(\exists y)$ 的作用域是 $R(x, y)$, x, y 都是约束变元。

c) $(\forall x)$ 和 $(\forall y)$ 的作用域是 $(P(x, y)\wedge Q(y, z))$, 其中 x, y 是约束变元, z 是自由变元。$(\exists x)$ 的作用域是 $P(x, y)$, 其中 x 是约束变元, y 是自由变元。在整个公式中, x 是约束出现, y 既是约束出现又是自由出现, z 是自

由出现。

d) $(\forall x)$的作用域是$(P(x)\wedge(\exists x)Q(x,z)\rightarrow(\exists y)R(x,y))$，$x$和$y$都是约束变元，但$Q(x,z)$中的$x$是受$\exists x$的约束，而不是受$\forall x$的约束。$Q(x,y)$中的$x$，$y$是自由变元。

从约束变元的概念可以看出，$P(x_1, x_2, \cdots, x_n)$是n元谓词，它有n个相互独立的自由变元，若对其中k个变元进行约束则成为$n-k$元谓词，因此，谓词公式中如果没有自由变元出现，则该式就成为一个命题。例如，$(\forall x)P(x, y, z)$是二元谓词。$(\exists y)(\forall x)P(x, y, z)$是一元谓词。

为了避免由于变元的约束与自由同时出现，引起概念上的混乱，故可对约束变元进行换名。使得一个变元在一个公式中只呈一种形式出现，即呈自由出现或呈约束出现。

我们知道，一个公式的约束变元所使用的名称符号是无关紧要的。故：$(\forall x)P(x)$与$(\forall y)P(y)$具有相同的意义。设$A(x)$表示x不小于0，那么

$(\forall x)A(x)$表示一切x都使得x不小于0；

$(\forall y)A(y)$表示一切y都使得y不小于0；

$(\forall t)A(t)$表示一切t都使得t不小于0。

这三个命题在实数域中都表示假命题"一切实数均不小于0"。同理$(\exists x)P(x)$与$(\exists y)P(y)$意义亦相同。

为此，我们可以对公式α中的约束变元更改名称符号，这种遵守一定规则的更改，称为约束变元的换名。其规则为：

(1) 对于约束变元可以换名，其更改的变元名称范围是量词中的指导变元，以及该量词作用域中所出现的该变元，在公式的其余部份不变。

(2) 换名时一定要更改为作用域中没有出现的变元名称。

例题2 对$(\forall x)(P(x)\rightarrow R(x, y))\wedge Q(x, y)$换名。

解 可换名为：$(\forall z)(P(z)\rightarrow R(z, y))\wedge Q(x, y)$，但不能改名为：$(\forall y)(P(y)\rightarrow R(y, y))\wedge Q(x, y)$以及$(\forall z)(P(z)\rightarrow R(x, y))\wedge Q(x, y)$。因为后两种更改都将使公式中量词的约束范围有所变动。

对于公式中的自由变元，也允许更改，这种更改叫做代入。自

由变元的代入，亦需遵守一定的规则，这个规则叫做自由变元的代入规则，现说明如下：

(1) 对于谓词公式中的自由变元，可以作代入，代入时需对公式中出现该自由变元的每一处进行。

(2) 用以代入的变元与原公式中所有变元的名称不能相同。

例题 3 对 $(\exists x)(P(y) \wedge R(x, y))$ 代入。

解 对 y 施行代入，经代入后公式为

$$(\exists x)(P(z) \wedge R(x, z))$$

但是 $(\exists x)(P(x) \wedge R(x, x))$ 与 $(\exists x)(P(z) \wedge R(x, y))$

这两种代入都是与规则不符的。

需要指出，量词作用域中的约束变元，当论域的元素是有限时，客体变元的所有可能的取代是可枚举的。

设论域元素为 $a_1, a_2, \cdots, a_n$。

则 $(\forall x)A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)$

$(\exists x)A(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n)$

量词对变元的约束，往往与量词的次序有关。

例如 $(\forall y)(\exists x)(x<(y-2))$ 表示任何 y 均有 x，使得 $x<y-2$。$(\exists y)(\exists x)(x<(y-2))$ 表示存在 y 有 x，使得 $x<y-2$。

这些命题中的多个量词，我们约定从左到右的次序读出。需要注意的是量词次序不能颠倒，否则将与原命题意义不符。

2-4 习题

(1) 对下面每个公式指出约束变元和自由变元。

a) $(\forall x)P(x) \rightarrow P(y)$

b) $(\forall x)(P(x) \wedge Q(x)) \wedge (\exists x)S(x)$

c) $(\exists x)(\forall y)(P(x) \wedge Q(y)) \rightarrow (\forall x)R(x)$

d) $(\exists x)(\exists y)(P(x, y) \wedge Q(z))$

(2) 如果论域是集合 $\{a, b, c\}$，试消去下面公式中的量词。

a) $(\forall x)P(x)$

b) $(\forall x)R(x) \wedge (\forall x)S(x)$

c) $(\forall x)(P(x) \rightarrow Q(x))$

d) $(\forall x)\neg P(x) \vee (\forall x)P(x)$

(3) 寻求下列各式的真假值。

a) $(\forall x)(P(x) \vee Q(x))$其中 $P(x)$: $x=1$, $Q(x)$: $x=2$ 而且论域是$\{1, 2\}$。

b) $(\forall x)(P \to Q(x)) \vee R(a)$ 其中 P: $2>1$, $Q(x)$: $x \leqslant 3$, $R(x)$: $x>5$ 而 a: 5, 论域是 $\{-2, 3, 6\}$。

(4) 对下列谓词公式中的约束变元进行换名。

a) $\forall x \exists y(P(x, z) \to Q(y)) \rightleftarrows S(x, y)$

b) $(\forall x(P(x) \to (R(x) \vee Q(x))) \wedge \exists x R(x)) \to \exists z S(x, z)$

(5) 对下列谓词公式中的自由变元进行代入。

a) $(\exists y A(x, y) \to \forall x B(x, z)) \wedge \exists x \forall z C(x, y, z)$

b) $(\forall y P(x, y) \wedge \exists z Q(x, z)) \vee \forall x R(x, y)$

2-5 谓词演算的等价式与蕴含式

在谓词公式中常包含命题变元和客体变元，当客体变元由确定的客体所取代，命题变元用确定的命题所取代时，就称作对谓词公式赋值。一个谓词公式经过赋值以后，就成为具有确定真值 T 或 F 的命题。

定义 2-5.1 给定任何两个谓词公式 wff A 和 wff B，设它们有共同的个体域 E，若对 A 和 B 的任一组变元进行赋值，所得命题的真值相同，则称谓词公式 A 和 B 在 E 上是等价的，并记作：$A \Leftrightarrow B$

定义 2-5.2 给定任意谓词公式 wff A，其个体域为 E，对于 A 的所有赋值，wff A 都为真，则称 wff A 在 E 上是有效的（或永真的）。

定义 2-5.3 一个谓词公式 wff A，如果在所有赋值下都为假，则称该 wff A 为不可满足的。

定义 2-5.4 一个谓词公式 wff A，如果至少在一种赋值下为真，则称该 wff A 为可满足的。

有了谓词公式的等价和永真等概念，就可以讨论谓词演算的一些等价式和蕴含式。

(1) 命题公式的推广

在命题演算中，任一永真公式，其中同一命题变元，用同一公式取代时，其结果也是永真公式，我们可以把这个情况推广到谓词公式之中，当谓词演算中的公式代替命题演算中永真公式的变元时，所得的谓词公式即为有效公式，故命题演算中的等价公式表和蕴含式表都可推广到谓词演算中使用。例如

$$(\forall x)(P(x)\rightarrow Q(x))\Leftrightarrow(\forall x)(\neg P(x)\vee Q(x))$$

$$(\forall x)P(x)\vee(\exists y)R(x,y)$$
$$\Leftrightarrow\neg(\neg(\forall x)P(x)\wedge\neg(\exists y)R(x,y))$$

$$(\exists x)H(x,y)\wedge\neg(\exists x)H(x,y)\Leftrightarrow F$$

(2) 量词与联结词 $\neg$ 之间的关系

为了说明这个问题，我们先举例讨论。

例1 设 $P(x)$ 表示 x 今天来校上课，则 $\neg P(x)$ 表示 x 今天没有来校上课。

故不是所有人今天来上课与存在一些人今天没有来上课在意义上相同，即 $\neg(\forall x)P(x)\Leftrightarrow(\exists x)\neg P(x)$。又，不是存在一些人今天来上课与所有的人今天都没有来上课在意义上相同，即 $\neg(\exists x)P(x)\Leftrightarrow(\forall x)\neg P(x)$。

为此我们得到公式：

$$\neg(\forall x)P(x)\Leftrightarrow(\exists x)\neg P(x)$$
$$\neg(\exists x)P(x)\Leftrightarrow(\forall x)\neg P(x)$$

这里约定，出现在量词之前的否定，不是否定该量词，而是否定被量化了的整个命题。

对于量词的转化律，可在有限个体域上证明。

设个体域中的客体变元为 $a_1, a_2, \cdots, a_n$，则

$$\neg(\forall x)A(x)\Leftrightarrow\neg(A(a_1)\wedge A(a_2)\wedge\cdots\wedge A(a_n))$$
$$\Leftrightarrow\neg A(a_1)\vee\neg A(a_2)\vee\cdots\vee\neg A(a_n)$$
$$\Leftrightarrow(\exists x)\neg A(x)$$

$$\neg(\exists x)A(x)\Leftrightarrow\neg(A(a_1)\vee A(a_2)\vee\cdots\vee A(a_n))$$
$$\Leftrightarrow\neg A(a_1)\wedge\neg A(a_2)\wedge\cdots\wedge\neg A(a_n)$$
$$\Leftrightarrow(\forall x)\neg A(x)$$

对于无穷个体域的情况，量词转化律也能作相应的推广。

可以看到，当我们将量词前面的 $\neg$ 移到量词的后面去时，存在量词改为全称量词，全称量词改为存在量词，反之，如将量词后面的 $\neg$ 移到量词前面去时，也要作相应的改变，这种量词与 $\neg$ 的关系是普遍成立的。

(3) 量词作用域的扩张与收缩

量词的作用域中，常有合取或析取项，如果其中为一个命题，则可将该命题移至量词作用域之外。如：

$$(\forall x)(A(x)\vee B)\Leftrightarrow((\forall x)A(x)\vee B)$$
$$(\forall x)(A(x)\wedge B)\Leftrightarrow((\forall x)A(x)\wedge B)$$
$$(\exists x)(A(x)\vee B)\Leftrightarrow((\exists x)A(x)\vee B)$$
$$(\exists x)(A(x)\wedge B)\Leftrightarrow((\exists x)A(x)\wedge B)$$

这是因为在 B 中不出现约束变元 x，故它属于或不属于量词的作用域均有同等意义。

从上述几个式子，我们还可推得如下几个式子。

$$((\forall x)A(x)\rightarrow B)\Leftrightarrow(\exists x)(A(x)\rightarrow B)$$
$$((\exists x)A(x)\rightarrow B)\Leftrightarrow(\forall x)(A(x)\rightarrow B)$$
$$(B\rightarrow(\forall x)A(x))\Leftrightarrow(\forall x)(B\rightarrow A(x))$$
$$(B\rightarrow(\exists x)A(x))\Leftrightarrow(\exists x)(B\rightarrow A(x))$$

例2 证明 $((\forall x)A(x)\rightarrow B)\Leftrightarrow(\exists x)(A(x)\rightarrow B)$

证明

$$\begin{aligned}((\forall x)A(x)\rightarrow B)&\Leftrightarrow\neg(\forall x)A(x)\vee B\\&\Leftrightarrow(\exists x)(\neg A(x))\vee B\\&\Leftrightarrow(\exists x)(\neg A(x)\vee B)\\&\Leftrightarrow(\exists x)(A(x)\rightarrow B)\end{aligned}$$

当谓词的变元与量词的指导变元不同时，亦能有类似于上述的公式。例如

$$(\forall x)(P(x)\vee Q(y))\Leftrightarrow((\forall x)P(x)\vee Q(y))$$
$$(\forall x)((\forall y)P(x,y)\wedge Q(z))\Leftrightarrow((\forall x)(\forall y)P(x,y)\wedge Q(z))$$

(4) 量词与命题联结词之间的一些等价式

量词与命题联结词之间存在不同的结合情况，下面举例说明

一些等价公式。

例如　联欢会上所有人既唱歌又跳舞和联欢会上所有人唱歌且所有人跳舞。这两个语句意义相同。故有

$$(\forall x)(A(x)\wedge B(x))\Leftrightarrow(\forall x)A(x)\wedge(\forall x)B(x)$$

根据上式亦有：

$$(\forall x)(\neg A(x)\wedge\neg B(x))\Leftrightarrow(\forall x)(\neg A(x))\wedge(\forall x)(\neg B(x))$$

故　$\neg(\exists x)(A(x)\vee B(x))\Leftrightarrow\neg((\exists x)A(x)\vee(\exists x)B(x))$

即　$(\exists x)(A(x)\vee B(x))\Leftrightarrow(\exists x)A(x)\vee(\exists x)B(x)$

(5) 量词与命题联结词之间的一些蕴含式

量词与命题联结词之间存在一些不同的结合情况，有些是蕴含公式。

例如　这些学生都聪明或这些学生都努力，可以推出这些学生都聪明或努力。但是这些学生都聪明或努力却不能推出这些学生都聪明或这些学生都努力。故有

$$(\forall x)A(x)\vee(\forall x)B(x)\Rightarrow(\forall x)(A(x)\vee B(x))$$

由上式可得

$$(\forall x)(\neg A(x))\vee(\forall x)(\neg B(x))\Rightarrow(\forall x)(\neg A(x)\vee\neg B(x))$$

即　$\neg((\exists x)A(x)\wedge(\exists x)B(x))$

$$\Rightarrow\neg(\exists x)(A(x)\wedge B(x))$$

因此有

$$(\exists x)(A(x)\wedge B(x))\Rightarrow(\exists x)A(x)\wedge(\exists x)B(x)$$

类似地有

$$(\forall x)(A(x)\rightarrow B(x))\Rightarrow(\forall x)A(x)\rightarrow(\forall x)B(x)$$

$$(\forall x)(A(x)\rightleftarrows B(x))\Rightarrow(\forall x)A(x)\rightleftarrows(\forall x)B(x)$$

上述这些等价式或蕴含式，很多可以互相推导，现将常用的式子列入表 2-5.1 中。

(6) 多个量词的使用

为了方便，我们只举两个量词的情况，更多量词的使用方法和它们类似。对于二元谓词如果不考虑自由变元，可以有以下八种情况。

表 2-5.1

E_{25}	$(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$
E_{26}	$(\forall x)(A(x) \wedge B(x)) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x)$
E_{27}	$\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$
E_{28}	$\neg(\forall x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
E_{29}	$(\forall x)(A \vee B(x)) \Leftrightarrow A \vee (\forall x)B(x)$
E_{30}	$(\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$
E_{31}	$(\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (\forall x)A(x) \rightarrow (\exists x)B(x)$
E_{32}	$(\forall x)A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$
E_{33}	$(\exists x)A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$
E_{34}	$A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$
E_{35}	$A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$
I_{15}	$(\forall x)A(x) \vee (\forall x)B(x) \Rightarrow (\forall x)(A(x) \vee B(x))$
I_{16}	$(\exists x)(A(x) \wedge B(x)) \Rightarrow (\exists x)A(x) \wedge (\exists x)B(x)$
I_{17}	$(\exists x)A(x) \rightarrow (\forall x)B(x) \Rightarrow (\forall x)(A(x) \rightarrow B(x))$

$$(\forall x)(\forall y)A(x, y) \qquad (\forall y)(\forall x)A(x, y)$$

$$(\exists x)(\exists y)A(x, y) \qquad (\exists y)(\exists x)A(x, y)$$

$$(\forall x)(\exists y)A(x, y) \qquad (\exists y)(\forall x)A(x, y)$$

$$(\forall y)(\exists x)A(x, y) \qquad (\exists x)(\forall y)A(x, y)$$

例如　设 $A(x, y)$ 表示 x 和 y 同姓，论域 x 是甲村的人，y 是乙村的人，则

$(\forall x)(\forall y)A(x, y)$：甲村与乙村所有的人都同姓。

$(\forall y)(\forall x)A(x, y)$：乙村与甲村所有的人都同姓。

显然上述两个语句的含义是相同的。故

$$(\forall x)(\forall y)A(x, y) \Leftrightarrow (\forall y)(\forall x)A(x, y)$$

同理　$(\exists x)(\exists y)A(x, y)$：甲村与乙村有人同姓。

$(\exists y)(\exists x)A(x, y)$：乙村与甲村有人同姓。

这两个语句的含义也相同。故

$$(\exists x)(\exists y)A(x, y) \Leftrightarrow (\exists y)(\exists x)A(x, y)$$

但是，$(\forall x)(\exists y)A(x, y)$ 表示对于甲村所有人，乙村都有人和他同姓。

$(\exists y)(\forall x)A(x, y)$ 表示存在一个乙村的人，甲村的人和他同姓。

$(\forall y)(\exists x)A(x, y)$ 表示对于乙村所有的人，甲村都有人与他同姓。

$(\exists x)(\forall y)A(x, y)$ 表示存在一个甲村的人，乙村的人都和他同姓。

上述四种语句，表达的情况各不相同，故全称量词与存在量词在公式中出现的次序，不能随意更换。具有两个量词的谓词公式，有如下一些蕴含关系。

$$(\forall x)(\forall y)A(x, y) \Rightarrow (\exists y)(\forall x)A(x, y)$$
$$(\forall y)(\forall x)A(x, y) \Rightarrow (\exists x)(\forall y)A(x, y)$$
$$(\exists y)(\forall x)A(x, y) \Rightarrow (\forall x)(\exists y)A(x, y)$$
$$(\exists x)(\forall y)A(x, y) \Rightarrow (\forall y)(\exists x)A(x, y)$$
$$(\forall x)(\exists y)A(x, y) \Rightarrow (\exists y)(\exists x)A(x, y)$$
$$(\forall y)(\exists x)A(x, y) \Rightarrow (\exists x)(\exists y)A(x, y)$$

2-5 习题

(1) 考虑以下赋值，

论域 $D=\{1, 2\}$

指定常数 a 和 b

a	b
1	2

指定函数 f

$f(1)$	$f(2)$
2	1

指定谓词 P

$P(1, 1)$	$P(1, 2)$	$P(2, 1)$	$P(2, 2)$
T	T	F	F

求以下各公式的真值。

a) $P(a, f(a)) \wedge P(b, f(b))$

b) $(\forall x)(\exists y)P(y, x)$

c) $(\forall x)(\forall y)(P(x, y) \to P(f(x), f(y)))$

(2) 对以下各公式赋值后求真值。

a) $(\forall x)(P(x) \to Q(f(x), a))$

b) $(\exists x)(P(f(x)) \wedge Q(x, f(a)))$

c) $(\exists x)(P(x) \wedge Q(x, a))$

d) $(\forall x)(\exists y)(P(x) \wedge Q(x, y))$

其中，论域 $D=\{1, 2\}$，$a=1$

$f(1)$	$f(2)$
2	1

$P(1)$	$P(2)$
F	T

$Q(1, 1)$	$Q(1, 2)$	$Q(2, 1)$	$Q(2, 2)$
T	T	F	F

(3) 举例说明下列各蕴含式。

a) $\neg((\exists x)P(x) \wedge Q(a)) \Rightarrow (\exists x)P(x) \to \neg Q(a)$

b) $(\forall x)(\neg P(x) \to Q(x))$, $(\forall x)\neg Q(x) \Rightarrow P(a)$

c) $(\forall x)(P(x) \to Q(x))$, $(\forall x)(Q(x) \to R(x)) \Rightarrow (\forall x)(P(x) \to R(x))$

d) $(\forall x)(P(x) \vee Q(x))$, $(\forall x)\neg P(x) \Rightarrow (\exists x)Q(x)$

e) $(\forall x)(P(x) \vee Q(x))$, $(\forall x)\neg P(x) \Rightarrow (\forall x)Q(x)$

(4) 求证　$(\exists x)(A(x) \to B(x)) \Leftrightarrow (\forall x)A(x) \to (\exists x)B(x)$

(5) 求证　$(\forall x)A(x) \vee (\forall x)B(x) \Rightarrow (\forall x)(A(x) \vee B(x))$

(6) 判断下列推证是否正确。

$$
\begin{aligned}
(\forall x)(A(x) \to B(x)) &\Leftrightarrow (\forall x)(\neg A(x) \vee B(x)) \\
&\Leftrightarrow (\forall x)\neg(A(x) \wedge \neg B(x)) \\
&\Leftrightarrow \neg(\exists x)(A(x) \wedge \neg B(x)) \\
&\Leftrightarrow \neg((\exists x)A(x) \wedge (\exists x)\neg B(x)) \\
&\Leftrightarrow \neg(\exists x)A(x) \vee \neg(\exists x)\neg B(x) \\
&\Leftrightarrow \neg(\exists x)A(x) \vee (\forall x)B(x) \\
&\Leftrightarrow (\exists x)A(x) \to (\forall x)B(x)
\end{aligned}
$$

(7) 求证　$(\forall x)(\forall y)(P(x) \to Q(y)) \Leftrightarrow (\exists x)P(x) \to (\forall y)Q(y)$

2-6 前束范式

在命题演算中，常常要将公式化成规范形式，对于谓词演算，也有类似情况，一个谓词演算公式，可以化为与它等价的范式。

定义 2-6.1 一个公式，如果量词均在全式的开头，它们的作用域，延伸到整个公式的末尾，则该公式叫做前束范式。

前束范式可记为下述形式：

$(\square v_1)(\square v_2)\cdots(\square v_n)A$，其中□可能是量词∀或量词∃，$v_i(i=1, 2, \cdots, n)$是客体变元，$A$是没有量词的谓词公式。

例如 $(\forall x)(\forall y)(\exists z)(Q(x,y)\rightarrow R(z))$，$(\forall y)(\forall x)(\neg P(x, y)\rightarrow Q(y))$等都是前束范式。

定理 2-6.1 任意一个谓词公式，均和一个前束范式等价。

证明 首先利用量词转化公式，把否定深入到命题变元和谓词填式的前面，其次利用$(\forall x)(A\vee B(x))\Leftrightarrow A\vee(\forall x)B(x)$和$(\exists x)(A\wedge B(x))\Leftrightarrow A\wedge(\exists x)B(x)$把量词移到全式的最前面，这样便得到前束范式。 □

例题 1 把公式$(\forall x)P(x)\rightarrow(\exists x)Q(x)$转化为前束范式。

解 $(\forall x)P(x)\rightarrow(\exists x)Q(x)\Leftrightarrow(\exists x)\neg P(x)\vee(\exists x)Q(x)$

$\Leftrightarrow(\exists x)(\neg P(x)\vee Q(x))$

例题 2 化公式$(\forall x)(\forall y)((\exists z)(P(x, z)\wedge P(y, z))\rightarrow(\exists u)Q(x, y, u))$为前束范式。

解 原式$\Leftrightarrow(\forall x)(\forall y)(\neg(\exists z)(P(x, z)\wedge P(y, z))\vee(\exists u)Q(x, y, u))$

$\Leftrightarrow(\forall x)(\forall y)((\forall z)(\neg P(x,z)\vee\neg P(y,z))\vee(\exists u)Q(x, y, u))$

$\Leftrightarrow(\forall x)(\forall y)(\forall z)(\exists u)(\neg P(x, z)\vee\neg P(y, z)\vee Q(x, y, u))$

例题 3 把公式$\neg(\forall x)\{(\exists y)A(x, y)\rightarrow(\exists x)(\forall y)[B(x, y)\wedge(\forall y)(A(y, x)\rightarrow B(x, y))]\}$化为前束范式。

解 第一步否定深入

原式$\Leftrightarrow(\exists x)\neg\{\neg(\exists y)A(x, y)\vee(\exists x)(\forall y)[B(x, y)\wedge(\forall y)(A(y, x)\rightarrow B(x, y))]\}$

$\Leftrightarrow(\exists x)\{(\exists y)A(x, y)\wedge(\forall x)(\exists y)[\neg B(x, y)\vee$
$(\exists y)\neg(A(y, x)\to B(x, y))]\}$

第二步改名，以便把量词提到前面。

$\Leftrightarrow(\exists x)\{(\exists y)A(x, y)\wedge(\forall u)(\exists R)[\neg B(u, R)\vee$
$(\exists z)\neg(A(z, u)\to B(u, z))]\}$

$\Leftrightarrow(\exists x)(\exists y)(\forall u)(\exists R)(\exists z)\{A(x, y)\wedge[\neg B(u, R)$
$\vee\neg(A(z, u)\to B(u, z))]\}$

定义 2-6.2 一个 wff A 如果具有如下形式称为前束合取范式。

$$(\square v_1)(\square v_2)\cdots(\square v_n)(A_{11}\vee A_{12}\vee\cdots\vee A_{1l_1})\wedge(A_{21}\vee A_{22}\vee\cdots\vee A_{2l_2})\wedge\cdots\wedge(A_{m1}\vee A_{m2}\vee\cdots\vee A_{ml_m})$$

其中 $\square$ 可能是量词 $\forall$ 或 $\exists$，$v_i(i=1, 2, \cdots, n)$是客体变元，A_{ij} 是原子公式或其否定。

例如公式

$$(\forall x)(\exists z)(\forall y)\{[\neg P\vee(x\neq a)\vee(z=b)]\wedge[Q(y)\vee(a=b)]\}$$

是前束合取范式。

定理 2-6.2 每一个 wff A 都可转化为与其等价的前束合取范式。(证明略) $\square$

我们用一个例子来说明这个定理。

例题 4 将 wff D: $(\forall x)[(\forall y)P(x)\vee(\forall z)q(z, y)\to\neg(\forall y)R(x, y)]$ 化为与它等价的前束合取范式。

解 第一步取消多余量词

$$D\Leftrightarrow(\forall x)[P(x)\vee(\forall z)q(z, y)\to\neg(\forall y)R(x, y)]$$

第二步换名

$$D\Leftrightarrow(\forall x)[P(x)\vee(\forall z)q(z, y)\to\neg(\forall w)R(x, w)]$$

第三步消去条件联结词

$$D\Leftrightarrow(\forall x)[\neg(P(x)\vee(\forall z)q(z, y))\vee\neg(\forall w)R(x, w)]$$

第四步将 $\neg$ 深入

$$D\Leftrightarrow(\forall x)[(\neg P(x)\wedge(\exists z)\neg q(z, y))\vee(\exists w)\neg R(x, w)]$$

第五步将量词推到左边

$$D\Leftrightarrow(\forall x)(\exists z)(\exists w)[(\neg P(x)\wedge\neg q(z, y))\vee\neg R(x, w)]$$
$$\Leftrightarrow(\forall x)(\exists z)(\exists w)[(\neg P(x)\vee\neg R(x, w))\wedge(\neg q(z, y)\vee\neg R(x, w))]$$

定义 2-6.8 一个 wff A 如具有如下形式则称为前束析取范式。

$$(\Box v_1)(\Box v_2)\cdots(\Box v_m)[A_{11}\wedge A_{12}\wedge\cdots\wedge A_{1l_1}]\vee[A_{21}\wedge A_{22}\wedge\cdots\wedge A_{2l_2}]\vee\cdots\vee[A_{m1}\wedge A_{m2}\wedge\cdots\wedge A_{ml_m}]$$

其中 □、v_i 与 A_{ij} 的概念与定义 2-6.2 中相同。

定理 2-6.8 每一个 wff A 都可以转换为与它等价的前束析取范式。(证明略) □

任一个 wff A 转换为等价的前束析取范式的步骤与例题 4 类同。

2-6 习题

(1) 把以下各式化为前束范式。

a) $(\forall x)(P(x)\to(\exists y)Q(x,y))$

b) $(\exists x)(\neg((\exists y)P(x,y))\to((\exists z)Q(z)\to R(x)))$

c) $(\forall x)(\forall y)(((\exists z)P(x,y,z)\wedge(\exists u)Q(x,u))\to(\exists v)Q(y,v)))$

(2) 求等价于下面 wff 的前束合取范式与前束析取范式。

a) $((\exists x)P(x)\vee(\exists x)Q(x))\to(\exists x)(P(x)\vee Q(x))$

b) $(\forall x)(P(x)\to(\forall y)((\forall z)Q(x,y)\to\neg(\forall z)R(y,x)))$

c) $(\forall x)P(x)\to(\exists x)((\forall z)Q(x,z)\vee(\forall z)R(x,y,z))$

d) $(\forall x)(P(x)\to Q(x,y))\to((\exists y)P(y)\wedge(\exists z)Q(y,z))$

2-7 谓词演算的推理理论

谓词演算的推理方法,可以看作是命题演算推理方法的扩张。因为谓词演算的很多等价式和蕴含式,是命题演算有关公式的推广,所以命题演算中的推理规则,如 P、T 和 CP 规则等亦可在谓词的推理理论中应用,但是在谓词推理中,某些前提与结论可能是受量词限制的,为了使用这些等价式和蕴含式,必须在推理过程中有消去和添加量词的规则,以便使谓词演算公式的推理过程可类似于命题演算中推理理论那样进行。现介绍如下规则。

(1) 全称指定规则，它表示为 US

$$\frac{(\forall x)P(x)}{\therefore\quad P(c)}$$

这里 P 是谓词，而 c 是论域中某个任意的客体。例如设论域为全人类。$P(x)$ 表示"x 总是要死的"，如果我们有 $(\forall x)P(x)$ 即是"所有人总是要死的"，那么全称指定规则可有结论"苏格拉底总是要死的"。

(2) 全称推广规则，它表示为 UG

$$\frac{P(x)}{\therefore\quad (\forall x)P(x)}$$

这个规则是要对命题量化，如果能够证明对论域中每一个客体 c 断言 $P(c)$ 都成立，则全称推广规则可得到结论 $(\forall x)P(x)$ 成立。在应用本规则时，必须能够证明前提 $P(x)$ 对论域中每一可能的 x 是真。

(3) 存在指定规则，它可表示为 ES

$$\frac{(\exists x)P(x)}{\therefore\quad P(c)}$$

这里 c 是论域中的某些客体，必须注意，应用存在指定规则，其指定的客体 c 不是任意的。例如 $(\exists x)P(x)$ 和 $(\exists x)Q(x)$ 都真，则对于某些 c 和 d，可以断定 $P(c)\wedge Q(d)$ 必定为真，但不能断定 $P(c)\wedge Q(c)$ 是真。

(4) 存在推广规则，它表示为 EG

$$\frac{P(c)}{\therefore\quad (\exists x)P(x)}$$

这里 c 是论域中的一个客体，这个规则比较明显，对于某些客体 c，若 $P(c)$ 为真，则在论域中必有 $(\exists x)P(x)$ 为真。

例题 1 证明 $(\forall x)(H(x)\rightarrow M(x))\wedge H(s)\Rightarrow M(s)$ 这是著名的苏格拉底论证。

其中 $H(x)$：x 是一个人。

$M(x)$：x 是要死的。

s: 苏格拉底。

证明(1) $(\forall x)(H(x)\rightarrow M(x))$ P

(2) $H(s)\rightarrow M(s)$ $US(1)$

(3) $H(s)$ P

(4) $M(s)$ $T(2)(3)\ I$

例题 2 证明 $(\forall x)(C(x)\rightarrow W(x)\wedge R(x))\wedge(\exists x)(C(x)\wedge Q(x))$
$\Rightarrow(\exists x)(Q(x)\wedge R(x))$

证明(1) $(\forall x)(C(x)\rightarrow W(x)\wedge R(x))$ P

(2) $(\exists x)(C(x)\wedge Q(x))$ P

(3) $C(a)\wedge Q(a)$ $ES(2)$

(4) $C(a)\rightarrow W(a)\wedge R(a)$ $US(1)$

(5) $C(a)$ $T(3)\ I$

(6) $W(a)\wedge R(a)$ $T(4)(5)\ I$

(7) $Q(a)$ $T(3)\ I$

(8) $R(a)$ $T(6)$

(9) $Q(a)\wedge R(a)$ $T(7)(8)\ I$

(10) $(\exists x)(Q(x)\wedge R(x))$ EG

注意本例推导过程中第(3)与(4)两条次序不能颠倒，若先用 US 规则得到 $C(a)\rightarrow W(a)\wedge R(a)$，则再用 ES 规则时，不一定得到 $C(a)\wedge Q(a)$，一般地应为 $C(b)\wedge Q(b)$，故无法推证下去。

例题 3 证明 $(\forall x)(P(x)\vee Q(x))\Rightarrow(\forall x)P(x)\vee(\exists x)Q(x)$

证法1把 $\neg((\forall x)P(x)\vee(\exists x)Q(x))$ 作为附加前提

(1) $\neg((\forall x)P(x)\vee(\exists x)Q(x))$ P

(2) $\neg(\forall x)P(x)\wedge\neg(\exists x)Q(x)$ $T(1)E$

(3) $\neg(\forall x)P(x)$ $T(2)I$

(4) $(\exists x)\neg P(x)$ $T(3)E$

(5) $\neg(\exists x)Q(x)$ $T(2)I$

(6) $(\forall x)\neg Q(x)$ $T(5)E$

(7) $\neg P(c)$ $ES(4)$

(8) $\neg Q(c)$ $US(6)$

(9) $\neg P(c)\wedge\neg Q(c)$ $T(7)(8)I$

(10) $\neg(P(c)\vee Q(c))$ $T(9)E$

(11) $(\forall x)(P(x)\vee Q(x))$ P

(12) $P(c)\vee Q(c)$ US

(13) $\neg(P(c)\vee Q(c))\wedge(P(c)\vee Q(c))$ 　　T(10)(12)I 矛盾

证法 2 本题可用 CP 规则，原题为

$(\forall x)(P(x)\vee Q(x))\Rightarrow\neg(\forall x)P(x)\rightarrow(\exists x)Q(x)$

(1)	$\neg(\forall x)P(x)$	P(附加前提)
(2)	$(\exists x)\neg P(x)$	T(1)E
(3)	$\neg P(c)$	ES(2)
(4)	$(\forall x)(P(x)\vee Q(x))$	P
(5)	$P(c)\vee Q(c)$	US(4)
(6)	$Q(c)$	T(3)(5)I
(7)	$(\exists x)Q(x)$	EG(6)
(8)	$\neg(\forall x)P(x)\rightarrow(\exists x)Q(x)$	CP

例题 4 　任何人违反交通规则，则要受到罚款，因此，如果没有罚款，则没有人违反交通规则。

解 　设 $S(x,y)$: 　“x 违反 y。” 　x 的论域为”人”。

$M(y)$: 　“y 是交通规则。”

$P(z)$: 　“z 是罚款。”

$R(x,z)$: 　“x 受到 z。”

故假设与结论可符号化地表示为：

H: $(\forall x)((\exists y)(S(x,y)\wedge M(y))\rightarrow(\exists z)(P(z)\wedge R(x,z)))$

C: $\neg(\exists z)P(z)\rightarrow(\forall x)(\forall y)(S(x,y)\rightarrow\neg M(y))$

因为结论是条件式，故我们可用 CP 规则进行推理，下面推导是否严格？

(1)	$(\forall x)((\exists y)(S(x,y)\wedge M(y))\rightarrow(\exists z)(P(z)\wedge R(x,z)))$	P
(2)	$(\exists y)(S(b,y)\wedge M(y))\rightarrow(\exists z)(P(z)\wedge R(b,z))$	US(1)
(3)	$\neg(\exists z)P(z)$	P(附加前提)
(4)	$(\forall z)\neg P(z)$	T(3)E
(5)	$\neg P(a)$	US(4)
(6)	$\neg P(a)\vee\neg R(b,a)$	T(5)I
(7)	$(\forall z)(\neg P(z)\vee\neg R(b,z))$	UG(6)
(8)	$\neg(\exists z)(P(z)\wedge R(b,z))$	$T(\neg)E$
(9)	$\neg(\exists y)(S(b,y)\wedge M(y))$	T(2)(8)I
(10)	$(\forall y)(\neg S(b,y)\vee\neg M(y))$	T(2)E
(11)	$(\forall y)(S(b,y)\rightarrow\neg M(y))$	T(10)E
(12)	$(\forall x)(\forall y)(S(x,y)\rightarrow\neg M(y))$	UG(11)
(13)	$\neg(\exists z)P(z)\rightarrow(\forall x)(\forall y)(S(x,y)\rightarrow\neg M(y))$	CP

2-7 习题

(1) 证明下列各式。

a) $(\forall x)(\neg A(x) \rightarrow B(x)),\ (\forall x)\neg B(x) \Rightarrow (\exists x)A(x)$

b) $(\exists x)A(x) \rightarrow (\forall x)B(x) \Rightarrow (\forall x)(A(x) \rightarrow B(x))$

c) $(\forall x)(A(x) \rightarrow B(x)),\ (\forall x)(C(x) \rightarrow \neg B(x))$
$\Rightarrow (\forall x)(C(x) \rightarrow \neg A(x))$

d) $(\forall x)(A(x) \vee B(x)),\ (\forall x)(B(x) \rightarrow \neg C(x)),\ (\forall x)C(x)$
$\Rightarrow (\forall x)A(x)$

(2) 用 CP 规则证明

a) $(\forall x)(P(x) \rightarrow Q(x)) \Rightarrow (\forall x)P(x) \rightarrow (\forall x)Q(x)$

b) $(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x)P(x) \vee (\exists x)Q(x)$

(3) 符号化下列命题并推证其结论。

a) 所有有理数是实数，某些有理数是整数，因此某些实数是整数。

b) 任何人如果他喜欢步行，他就不喜欢乘汽车，每一个人或者喜欢乘汽车或者喜欢骑自行车。有的人不爱骑自行车，因而有的人不爱步行。

c) 每个大学生不是文科学生就是理工科学生，有的大学生是优等生，小张不是理工科学生，但他是优等生，因而如果小张是大学生，他就是文科学生。

第二篇 集合论

集合论是现代各科数学的基础，它的起源可以追溯到十六世纪末期。开始时为了追寻微积分的坚实的基础，人们仅进行了有关数集的研究。直到1876～1883年，康托尔(Georg Cantor)发表了一系列有关集合论的文章，对任意元素的集合进行了深入的探讨，提出了关于基数，序数和良序集等理论，奠定了集合论的深厚基础。但是随着集合论的发展，以及它与数学哲学密切联系所作的讨论，在1900年前后出现了各种悖论，使集合论的发展一度陷入僵滞的局面。1904～1908年，策墨罗(Zermelo)列出了第一个集合论的公理系统，他的公理，使数学哲学中产生的一些矛盾基本上得到统一，在此基础上以后就逐步形成了公理化集合论和抽象集合论，使该学科成为在数学中发展最为迅速的一个分支。现在集合论观点已渗透到古典分析、泛函、概率、函数论以及信息论、排队论等现代数学各个领域。本篇介绍集合论的基础知识如集合运算、性质、序偶、关系、函数、基数等。

第三章　集合与关系

3-1　集合的概念和表示法

集合是一个不能精确定义的基本概念。一般地说，把具有共同性质的一些东西，汇集成一个整体，就形成一个集合。例如：教室内的桌椅；图书馆的藏书；全国的高等学校；自然数的全体；直线上的点子等，均分别构成一个集合。通常用大写英文字母表示集合的名称；用小写英文字母表示组成集合的事物，即元素。若元素 a 属于集合 A，记作 $a\in A$，亦称 A 包含 a，或 a 在 A 之中，或 a 是 A 的成员。若元素 a 不属于 A，记作 $a\notin A$，亦称 A 不包含 a，或 a 不在 A 中，或 a 不是 A 的成员。一个集合，若其组成集合的元素个数是有限的，则称作有限集，否则就称作无限集。

说明集合的方法有两种：一种是将某集合的元素列举出来，称作列举法；例如：$A=\{a, b, c, d\}$，$B=\{1, 2, 3, \cdots\}$，$D=\{$桌子，灯泡，自然数，老虎$\}$，$C=\{2, 4, 6, \cdots, 2n\}$，$S=\{a, a^2, a^3, \cdots\}$等。

另一种是利用一项规则，以便决定某一物体是否属于该集合，称作叙述法，例如：

$$S_1=\{x|x\text{是正奇数}\},$$

$$S_2=\{x|x\text{是中国的省}\},$$

$$S_3=\{y|y=a\text{ 或 }y=b\}。$$

如果我们用 $p(x)$ 表示任何谓词，则 $\{x|p(x)\}$ 可表示集合。

设集合为 $A=\{x|p(x)\}$，如果 $p(b)$ 为真，那么 $b\in A$，否则 $b\notin A$。

两个集合相等是按照下述原理定义的。

外延性原理： 两个集合是相等的，当且仅当它们有相同的

成员。

两个集合 A 和 B 相等，记作 $A=B$，两个集合不相等，则记作 $A\neq B$。

集合的元素还可以允许是一个集合。例如：

$$S=\{a, \{1, 2\}, p, \{q\}\}$$

必须指出：$q\in\{q\}$，但 $q\notin S$，同理 $1\in\{1, 2\}$，但 $1\notin S$。

例如：设 A 是小于 10 的素数集合，即 $A=\{2, 3, 5, 7\}$，又设代数方程 $x^4-17x^3+101x^2-247x+210=0$ 的所有根可组成的集合为 B，则 B 正好也是 $\{2, 3, 5, 7\}$，因此这两个集合是相等的。

又如：$\{1, 2, 4\}=\{1, 2, 2, 4\}$

$\{1, 2, 4\}=\{1, 4, 2\}$

但 $\{\{1, 2\}, 4\}\neq\{1, 4, 2\}$

$\{1, 3, 5, \cdots\}=\{x \mid x\text{ 是正奇数}\}$

定义 3-1.1 设 A、B 是任意两个集合，假如 A 的每一个元素是 B 的成员，则称 A 为 B 的子集，或 A 包含在 B 内，或 B 包含 A。记作 $A\subseteq B$，或 $B\supseteq A$。

$$A\subseteq B\Leftrightarrow\forall x(x\in A\rightarrow x\in B)$$

例如：$A=\{1, 2, 3\}$，$B=\{1, 2\}$，$C=\{1, 3\}$，$D=\{3\}$，则 $B\subseteq A$，$C\subseteq A$，$D\subseteq A$，$D\subseteq C$。

根据子集的定义，显然有：

$A\subseteq A$ 自反性

$(A\subseteq B)\wedge(B\subseteq C)\Rightarrow(A\subseteq C)$ 传递性

定理 3-1.1 集合 A 和集合 B 相等的充分必要条件是这两个集合互为子集。

证明 设任意两集合相等，则根据定义，有相同的元素。故 $(\forall x)(x\in A\rightarrow x\in B)$ 为真，且 $(\forall x)(x\in B\rightarrow x\in A)$ 也为真，即 $A\subseteq B$ 且 $B\subseteq A$。

反之，若 $A\subseteq B$ 且 $B\subseteq A$，假设 $A\neq B$，则 A 与 B 的元素不完全相同，设有某一元素 $x\in A$ 但 $x\notin B$，这与 $A\subseteq B$ 条件相矛盾；或设某一元素 $x\in B$ 但 $x\notin A$，这就与 $B\subseteq A$ 条件相矛盾。故 A、B

的元素必须相同，即 $A=B$。 □

这个定理很重要，今后证明两个集合相等，主要利用这个互为子集的判定条件。

定义 3-1.2 如果集合 A 的每一个元素都属于 B，但集合 B 中至少有一个元素不属于 A，则称 A 为 B 的真子集，记作 $A\subset B$。

$$A\subset B\Leftrightarrow(\forall x)(x\in A\rightarrow x\in B)\wedge(\exists x)(x\in B\wedge x\notin A)$$

$$A\subset B\Leftrightarrow A\subseteq B\wedge A\neq B$$

例如，整数集是有理数集的真子集。

定义 3-1.3 不包含任何元素的集合是空集，记作 $\emptyset$。

$$\emptyset=\{x|p(x)\wedge\neg p(x)\},\quad p(x)\text{是任意谓词}$$

注意：$\emptyset\neq\{\emptyset\}$，但 $\emptyset\in\{\emptyset\}$。

定理 3-1.2 对于任意一个集合 A，$\emptyset\subseteq A$。

证明 假设 $\emptyset\subseteq A$ 是假，则至少有一个元素 x，使 $x\in\emptyset$ 且 $x\notin A$，因为空集 $\emptyset$ 不包含任何元素，所以这是不可能的。 □

根据空集和子集的定义，可以看到，对于每个非空集合 A，至少有两个不同的子集，A 和 $\emptyset$，即 $A\subseteq A$ 和 $\emptyset\subseteq A$，我们称 A 和 $\emptyset$ 是 A 的平凡子集。一般地说，A 的每个元素都能确定 A 的一个子集，即若 $a\in A$，则 $\{a\}\subseteq A$。

定义 3-1.4 在一定范围内，如果所有集合均为某一集合的子集，则称该集合为全集，记作 E。对于任一 $x\in A$，因 $A\subseteq E$，故 $x\in E$，即

$$(\forall x)(x\in E)\text{恒真}$$

故 $E=\{x|p(x)\vee\neg p(x)\}$，　$p(x)$为任何谓词

全集的概念相当于论域，如在初等数论中，全体整数组成了全集。在考虑某大学的部分学生组成的集合(如系，班级等)时，该大学的全体学生组成了全集。

设全集 $E=\{a, b, c\}$，它的所有可能的子集计有：$S_0=\emptyset$，$S_1=\{a\}$，$S_2=\{b\}$，$S_3=\{c\}$，$S_4=\{a, b\}$，$S_5=\{b, c\}$，$S_6=\{c, a\}$，$S_7=\{a, b, c\}$，这些子集都包含在 B 中，即 $S_i\subseteq E(i=0, 1, 2, \cdots, 7)$，但是 $S_i\notin E$。如果把 S_i 作为元素，将可以另外组成一种集合。

定义 3-1.5 给定集合 A，由集合 A 的所有子集为元素组成的集合，称为集合 A 的幂集，记为 $\mathscr{P}(A)$。

例如 $A=\{a, b, c\}$

$$\mathscr{P}(A)=\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$$

定理 3-1.3 如果有限集合 A 有 n 个元素，则其幂集 $\mathscr{P}(A)$ 有 2^n 个元素。

证明 A 的所有由 k 个元素组成的子集数为从 n 个元素中取 k 个的组合数。

$$C_n^k=\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$$

另外，因 $\emptyset\subseteq A$，故 $\mathscr{P}(A)$ 的总数 N 可表示为

$$N=1+C_n^1+C_n^2+\cdots+C_n^k+\cdots+C_n^n=\sum_{k=0}^{n}C_n^k$$

但又因 $$(x+y)^n=\sum_{k=0}^{n}C_n^k\cdot x^k\cdot y^{n-k}$$

令 $x=y=1$， $2^n=\sum_{k=0}^{n}C_n^k$

故 $\mathscr{P}(A)$ 的元素个数是 2^n。 □

现在我们引进一种编码，用来唯一地表示有限集幂集的元素，现以上面 $S=\{a, b, c\}$ 这个集合为例。

$$\mathscr{P}(S)=\{S_i|i\in J\} \qquad J=\{i|i \text{ 是二进制数且 } 000\leqslant i\leqslant 111\}$$

例如 $S_3=S_{011}=\{b, c\}$，$S_6=S_{110}=\{a, b\}$ 等。一般地 $\mathscr{P}(S)=\{S_0, S_1, \cdots, S_{2^n-1}\}$，即 $\mathscr{P}(S)=\{S_i|i\in J\}$，$J=\{i|i$ 是二进制数且 $\overbrace{000\cdots0}^{n}\leqslant i\leqslant\overbrace{111\cdots1}^{n}\}$。

3-1 习题

(1) 写出下列集合的表示式

a) 所有一元一次方程的解组成的集合。

b) x^6-1 在实数域中的因式集。

c) 直角坐标系中，单位圆内(不包括单位圆周)的点集。

d) 极坐标系中，单位圆外(不包括单位圆周)的点集。

e) 能被 5 整除的整数集。

(2) 设有某电视台，拟制定一项为时半小时的节目，其中包含戏剧、音乐与广告。每项节目都定为五分钟的倍数，试求

a) 各种时间分配情况的集合。

b) 戏剧所分配的时间较音乐多的集合。

c) 广告所分配的时间与音乐或戏剧所分配的时间相等的集合。

d) 音乐所分配的时间恰为五分钟的集合。

(3) 给出集合 A、B 和 C 的例子，使得 $A\in B$, $B\in C$, 和 $A\notin C$。

(4) 对任意集合 A、B、C，确定下列各命题是否为真，并证明之。

a) 如果 $A\in B$ 及 $B\subseteq C$, 则 $A\in C$

b) 如果 $A\in B$ 及 $B\subseteq C$, 则 $A\subseteq C$

c) 如果 $A\subseteq B$ 及 $B\in C$, 则 $A\in C$

d) 如果 $A\subseteq B$ 及 $B\in C$, 则 $A\subseteq C$

e) 如果 $A\in B$ 及 $B\nsubseteq C$, 则 $A\notin C$

f) 如果 $A\subseteq B$ 及 $B\in C$, 则 $A\notin C$

(5) $A\subseteq B$, $A\in B$ 是可能的吗？予以说明。

(6) 确定下列集合的幂集

a) $\{a, \{a\}\}$

b) $\{\{1, \{2, 3\}\}\}$

c) $\{\emptyset, a, \{b\}\}$

d) $\mathscr{P}(\emptyset)$

e) $\mathscr{P}(\mathscr{P}(\emptyset))$

(7) 设 $A=\{\emptyset\}$, $B=\mathscr{P}(\mathscr{P}(A))$。

a) 是否 $\emptyset\in B$? 是否 $\emptyset\subseteq B$?

b) 是否 $\{\emptyset\}\in B$? 是否 $\{\emptyset\}\subseteq B$?

c) 是否 $\{\{\emptyset\}\}\in B$? 是否 $\{\{\emptyset\}\}\subseteq B$?

(8) 证明若 a, b, c 和 d 是任意客体，则 $\{\{a\}, \{a, b\}\}=\{\{c\}, \{c, d\}\}$ 当且仅当 $a=c$ 和 $b=d$。

(9) 设某集合有 101 个元素。试问

a) 可构成多少个子集?

b) 其中有多少个子集的元素为奇数?

c) 是否会有 102 个元素的子集?

(10) 设 $S=\{a_1, a_2, \cdots, a_8\}$，$B_i$ 是 S 的子集，由 B_{17} 和 B_{31} 所表达的子集是什么？应如何规定子集 $\{a_2, a_6, a_7\}$ 和 $\{a_1, a_8\}$。

3-2 集合的运算

集合的运算，就是以给定集合为对象，按照确定的规则得到另外一些集合。

(1) 集合的交

定义 3-2.1 设任意两个集合 A 和 B，由集合 A 和 B 的所有共同元素组成的集合 S，称为 A 和 B 的交集，记作 $A\cap B$。

$$S=A\cap B=\{x\mid (x\in A)\wedge(x\in B)\}$$

交集的定义如图 3-2.1（文氏图）所示。

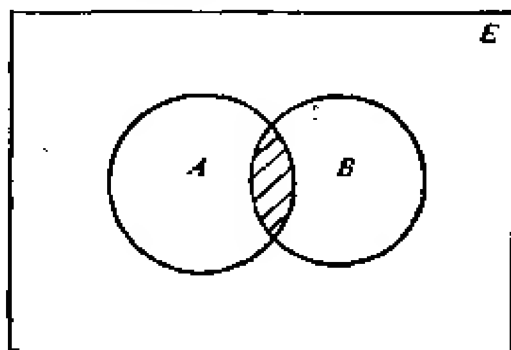


图 3-2.1

例 1 $A=\{0, 2, 4, 6, 8, 10, 12\}$

$B=\{1, 2, 3, 4, 5, 6\}$

$A\cap B=\{2, 4, 6\}$

例 2 设 A 是所有矩形的集合，B 是平面上所有菱形的集合，$A\cap B$ 是所有正方形的集合。

例 3 设 A 是所有被 K 除尽的整数的集合，B 是所有被 L 除尽的整数的集合，则 $A\cap B$ 是被 K 与 L 最小公倍数除得尽的整数的集合。

例题 1 设 $A\subseteq B$，求证 $A\cap C\subseteq B\cap C$

证明 若 $x\in A$ 则 $x\in B$，对任一 $x\in A\cap C$，则 $x\in A$ 且 $x\in C$ 即 $x\in B$ 且 $x\in C$，故 $x\in B\cap C$。因此，$A\cap C\subseteq B\cap C$。

集合的交运算具有以下性质：

a) $A\cap A=A$

b) $A\cap\emptyset=\emptyset$

c) $A\cap E=A$

d) $A\cap B=B\cap A$

e) $(A\cap B)\cap C=A\cap(B\cap C)$

现对 e) 证明如下：

证明　$(A\cap B)\cap C=\{x\mid(x\in A\cap B)\wedge(x\in C)\}$

$A\cap(B\cap C)=\{x\mid(x\in A)\wedge(x\in B\cap C)\}$

$$\begin{aligned}(x\in A\cap B)\wedge(x\in C)&\Leftrightarrow[(x\in A)\wedge(x\in B)]\wedge(x\in C)\\&\Leftrightarrow(x\in A)\wedge[(x\in B)\wedge(x\in C)]\\&\Leftrightarrow(x\in A)\wedge(x\in B\cap C)\end{aligned}$$

因此，$(A\cap B)\cap C\Leftrightarrow A\cap(B\cap C)$

此外，从交的定义还可以得到 $A\cap B\subseteq A$，$A\cap B\subseteq B$。

若集合 A、B 没有共同的元素，则可写为 $A\cap B=\emptyset$，此时亦称 A 与 B 不相交。

因为集合交的运算满足结合律，故 n 个集合 $A_1, A_2, \cdots, A_n$ 的交可记为：

$$P=A_1\cap A_2\cap\cdots\cap A_n=\bigcap_{i=1}^{n}A_i$$

例　$A_1=\{1, 2, 8\}$，$A_2=\{2, 8\}$，$A_3=\{4, 8\}$。则

$$\bigcap_{i=1}^{3}A_i=\{8\}$$

(2) 集合的并

定义 3-2.2　设任意两个集合 A 和 B，所有属于 A 或属于 B 的元素组成的集合 S，称为 A 和 B 的并集，记作 $A\cup B$。

$$S=A\cup B=\{x\mid(x\in A)\vee(x\in B)\}$$

并集的定义如图 3-2.2 所示。

例如，设 $A=\{1, 2, 3, 4\}$，$B=\{2, 4, 5\}$。则

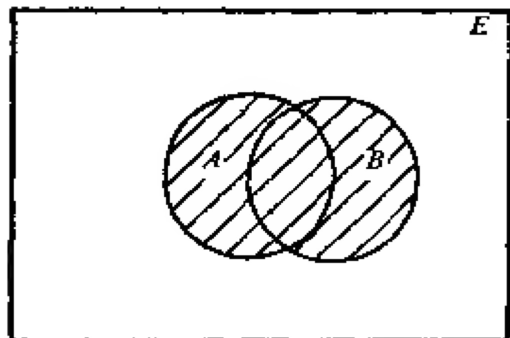


图 3-2.2

$$A\cup B=\{1, 2, 3, 4, 5\}$$

集合并的运算具有以下性质：

a) $A\cup A=A$

b) $A\cup E=E$

c) $A\cup\emptyset=A$

d) $A\cup B=B\cup A$

e) $(A\cup B)\cup C=A\cup(B\cup C)$

此外从并的定义还可以得到 $A\subseteq A\cup B$, $B\subseteq A\cup B$。

例题 2 设 $A\subseteq B$, $C\subseteq D$, 则 $A\cup C\subseteq B\cup D$

证明 对任意 $x\in A\cup C$,则有 $x\in A$ 或 $x\in C$。若 $x\in A$,由 $A\subseteq B$ 则 $x\in B$,故 $x\in B\cup D$;若 $x\in C$,由 $C\subseteq D$, 则 $x\in D$,故 $x\in B\cup D$,因此, $A\cup C\subseteq B\cup D$。

同理可证 $A\subseteq B\Rightarrow A\cup C\subseteq B\cup C$。

因为集合的并运算满足结合律, 故对于 n 个集合 A_1, A_2, $\cdots$, A_n 的并可记为:

$$W=A_1\cup A_2\cup\cdots\cup A_n=\bigcup_{i=1}^{n}A_i$$

例如,设 $A_1=\{1, 2, 3\}$, $A_2=\{3, 8\}$, $A_3=\{2, 6\}$, 则

$$\bigcup_{i=1}^{3}A_i=\{1, 2, 3, 6, 8\}$$

定理 3-2.1 设 A、B、C 为三个集合,则下列分配律成立。

a) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

b) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

证明 a) 设 $S=A\cap(B\cup C)$,$T=(A\cap B)\cup(A\cap C)$, 若 $x\in S$,则 $x\in A$ 且 $x\in B\cup C$, 即 $x\in A$ 且 $x\in B$ 或 $x\in A$ 且 $x\in C$, $x\in A\cap B$ 或 $x\in A\cap C$ 即 $x\in T$, 所以 $S\subseteq T$。

反之, 若 $x\in T$, 则 $x\in A\cap B$ 或 $x\in A\cap C$, $x\in A$ 且 $x\in B$ 或 $x\in A$ 且 $x\in C$, 即 $x\in A$ 且 $x\in B\cup C$, 于是 $x\in S$, 所以 $T\subseteq S$。因此 $T=S$。

b) 其证明完全与 a)类似。 □

定理 3-2.2 设 A、B 为任意两个集合,则下列关系式成立。

a) $A\cup(A\cap B)=A$

b) $A\cap(A\cup B)=A$

证明 a) $A\cup(A\cap B)=(A\cap E)\cup(A\cap B)$

$$=A\cap(E\cup B)=A$$

b) $A\cap(A\cup B)=(A\cup A)\cap(A\cup B)$

$$=A\cup(A\cap B)=A$$

这就是著名的吸收律。 □

定理 3-2.3 $A\subseteq B$，当且仅当 $A\cup B=B$ 或 $A\cap B=A$

证明 若 $A\subseteq B$，对任意 $x\in A$ 必有 $x\in B$，对任意 $x\in A\cup B$ 则 $x\in A$ 或 $x\in B$，即 $x\in B$，所以 $A\cup B\subseteq B$。又 $B\subseteq A\cup B$，故得到 $A\cup B=B$。反之，若 $A\cup B=B$，因为 $A\subseteq A\cup B$，故 $A\subseteq B$。

同理可证 $A\subseteq B$，iff $A\cap B=A$。 □

(3) 集合的补

定义 3-2.3 设 A、B 为任意两个集合，所有属于 A 而不属于 B 的一切元素组成的集合 S 称为 B 对于 A 的补集，或相对补，记作 $A-B$。

$$S=A-B=\{x|x\in A\wedge x\notin B\}=\{x|x\in A\wedge\urcorner(x\in B)\}$$

$A-B$ 也称集合 A 和 B 的差，定义如图 3-2.3 所示。

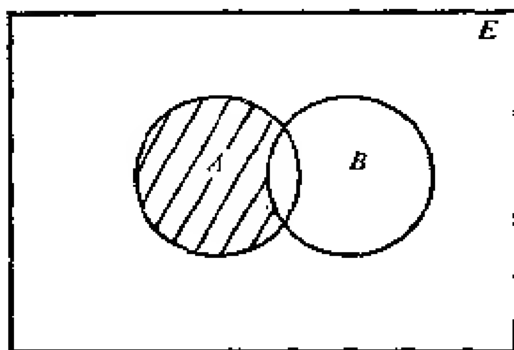


图 3-2.3

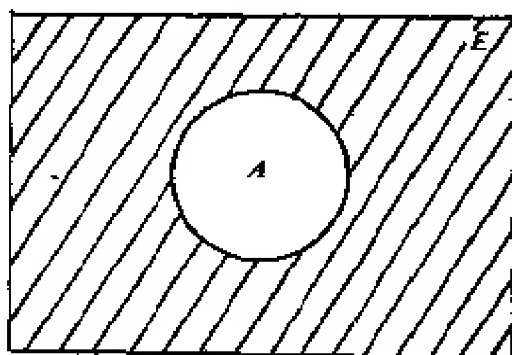


图 3-2.4

例题 3 设 $A=\{2, 5, 6\}$，$B=\{1, 2, 4, 7, 9\}$，求 $A-B$。

解 $A-B=\{5, 6\}$

例题 4 设 A 是素数集合，B 是奇数集合，求 $A-B$。

解 $A-B=\{2\}$

定义 3-2.4 设 E 为全集，对任一集合 A 关于 E 的补 $E-A$，称为集合 A 的绝对补，记作 $\sim A$。

$$\sim A=E-A=\{x|x\in E\wedge x\notin A\}$$

$\sim A$ 的定义如图 3-2.4 所示。

由补的定义可知：

a) $\sim(\sim A)=A$

b) $\sim E=\emptyset$

c) $\sim\emptyset=E$

d) $A\cup\sim A=E$

e) $A\cap\sim A=\emptyset$

定理 3-2.4 设 A、B 为任意两个集合，则下列关系式成立。

a) $\sim(A\cup B)=\sim A\cap\sim B$

b) $\sim(A\cap B)=\sim A\cup\sim B$

证明 a) $\sim(A\cup B)=\{x|x\in\sim(A\cup B)\}$

$$=\{x|x\notin A\cup B\}$$

$$=\{x|(x\notin A)\wedge(x\notin B)\}$$

$$=\{x|(x\in\sim A)\wedge(x\in\sim B)\}$$

$$=\sim A\cap\sim B$$

b) 其证法与 a) 类似。 □

定理 3-2.5 设 A、B 为任意两个集合，则下列关系式成立。

a) $A-B=A\cap\sim B$

b) $A-B=A-(A\cap B)$

证明 a) 从略。

b) 设 $x\in(A-B)$，即 $x\in A$ 且 $x\notin B$。因 $x\notin B$ 必有 $x\notin(B\cap A)$，故 $x\in[A-(B\cap A)]$，即 $A-B\subseteq[A-(B\cap A)]$。

又设 $x\in[A-(B\cap A)]$，则 $x\in A$ 且 $x\notin(B\cap A)$，即 $x\in A$ 且 $x\in\sim(A\cap B)$，$x\in A$ 且 $x\in\sim A$ 或 $x\in\sim B$，但 $x\in A$ 且 $x\in\sim A$ 是不可能的，故 $x\in A$ 且 $x\in\sim B$，$x\in A-B$，得到 $A-(A\cap B)\subseteq A-B$。因此 $A-B=A-(A\cap B)$。 □

定理 3-2.6 设 A、B、C 为三个集合，则

$$A\cap(B-C)=(A\cap B)-(A\cap C)$$

证明 $A\cap(B-C)=A\cap(B\cap\sim C)=A\cap B\cap\sim C$

又 $(A\cap B)-(A\cap C)=(A\cap B)\cap\sim(A\cap C)$

$$=(A\cap B)\cap(\sim A\cup\sim C)$$

$$=(A\cap B\cap\sim A)\cup(A\cap B\cap\sim C)$$

$$=\emptyset\cup(A\cap B\cap\sim C)=A\cap B\cap\sim C$$

因此，$A\cap(B-C)=(A\cap B)-(A\cap C)$ □

定理 3-2.7 设 A、B 为两个集合，若 $A\subseteq B$，则

a) $\sim B\subseteq\sim A$

b) $(B-A)\cup A=B$

证明 a) 若 $x\in A$，则 $x\in B$，因此 $x\notin B$ 必有 $x\notin A$，故 $x\in\sim B$ 必有 $x\in\sim A$，即 $\sim B\subseteq\sim A$。

b) $(B-A)\cup A=(B\cap\sim A)\cup A=(B\cup A)\cap(\sim A\cup A)$

$$=(B\cup A)\cap E=B\cup A$$

因为 $A\subseteq B$，就有 $B\cup A=B$。因此

$$(B-A)\cup A=B$$ □

(4) 集合的对称差

定义 3-2.5 设 A、B 为任意两个集合，A 和 B 的对称差为集合 S，其元素或属于 A，或属于 B，但不能既属于 A 又属于 B，记作 $A\oplus B$。

$$S=A\oplus B=(A-B)\cup(B-A)=\{x|x\in A\overline{\vee}x\in B\}$$

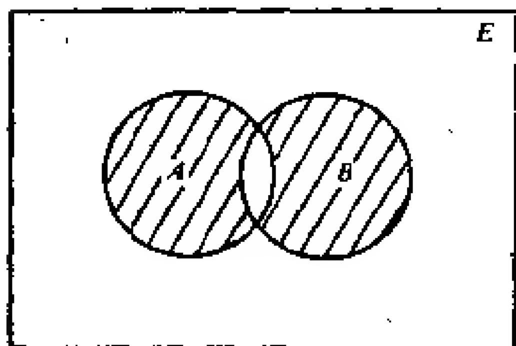


图 3-2.5

对称差的定义如图 3-2.5 所示。

由对称差的定义很易推得如下性质：

a) $A\oplus B=B\oplus A$

b) $A\oplus\emptyset=A$

c) $A\oplus A=\emptyset$

d) $A\oplus B=(A\cap\sim B)\cup(\sim A\cap B)$

e) $(A\oplus B)\oplus C=A\oplus(B\oplus C)$

证明 e) $(A\oplus B)\oplus C$

$$=((A\oplus B)\cap\sim C)\cup(\sim(A\oplus B)\cap C)$$

$$=[((A\cap\sim B)\cup(\sim A\cap B))\cap\sim C]$$

$$\cup[\sim((A\cap\sim B)\cup(\sim A\cap B))\cap C]$$

$$=(A\cap\sim B\cap\sim C)\cup(\sim A\cap B\cap\sim C)$$

$$\cup[((\sim A\cup B)\cap(A\cup\sim B))\cap C]$$

但 $[(\sim A\cup B)\cap(A\cup\sim B)]\cap C$

$= [((\sim A \cup B) \cap A) \cup ((\sim A \cup B) \cap \sim B)] \cap C$

$= ((\sim A \cap A) \cup (A \cap B) \cup (\sim A \cap \sim B)$

$\cup (B \cap \sim B)) \cap C$

$= (\emptyset \cup (A \cap B) \cup (\sim A \cap \sim B) \cup \emptyset) \cap C$

$= (A \cap B \cap C) \cup (\sim A \cap \sim B \cap C)$

故 $(A \oplus B) \oplus C$

$= (A \cap \sim B \cap \sim C) \cup (\sim A \cap B \cap \sim C)$

$\cup (A \cap B \cap C) \cup (\sim A \cap \sim B \cap C)$

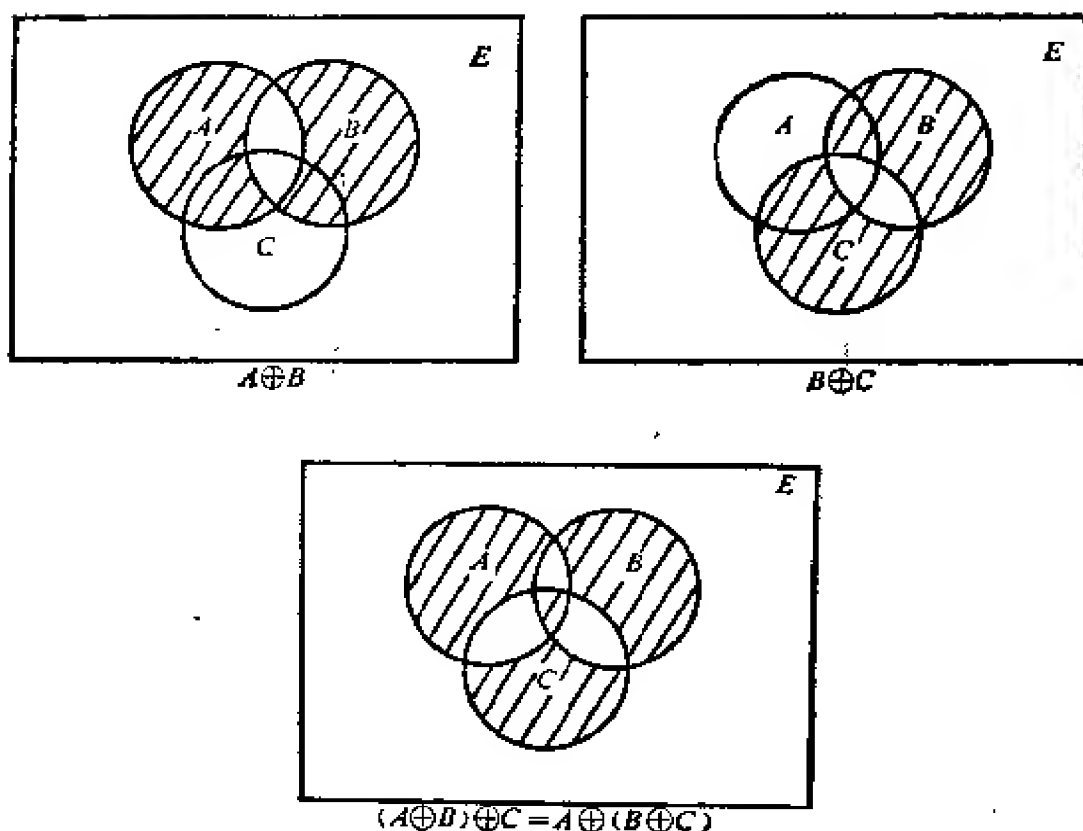


图 3-2.6

又 $A \oplus (B \oplus C)$

$= [A \cap \sim (B \oplus C)] \cup [\sim A \cap (B \oplus C)]$

$= [A \cap \sim ((B \cap \sim C) \cup (\sim B \cap C))]$

$\cup [\sim A \cap ((B \cap \sim C) \cup (\sim B \cap C))]$

$= [A \cap ((\sim B \cup C) \cap (B \cup \sim C)]$

$\cup [(\sim A \cap B \cap \sim C) \cup (\sim A \cap \sim B \cap C)]$

因为 $A \cap ((\sim B \cup C) \cap (B \cup \sim C))$

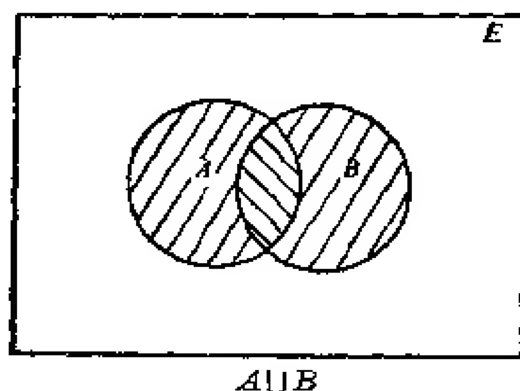
$$=A\cap[(\sim B\cap B)\cup(\sim B\cap\sim C)$$
$$\cup(C\cap B)\cup(C\cap\sim C)]$$
$$=A\cap[(\sim B\cap\sim C)\cup(C\cap B)]$$
$$=(A\cap\sim B\cap\sim C)\cup(A\cap C\cap B)$$

故 $A\oplus(B\oplus C)$

$$=(A\cap\sim B\cap\sim C)\cup(A\cap B\cap C)$$
$$\cup(\sim A\cap B\cap\sim C)\cup(\sim A\cap\sim B\cap C)$$

因此 $(A\oplus B)\oplus C=A\oplus(B\oplus C)$

对称差集的结合性亦可用图 3-2.6 说明。



$A\cup B$

图 3-2.7

从图 3-2.7 的文氏图亦可以看出下列关系式成立。

$$A\cup B=(A\cap\sim B)\cup(B\cap\sim A)\cup(A\cap B)$$
$$A\cup B=(A\oplus B)\cup(A\cap B)$$

3-2 习题

(1) 设 $A=\{x|x<5, x\in N\}$, $B=\{x|x<7, x$是正偶数$\}$, 求$A\cup B$, $A\cap B$。

(2) 设 $A=\{x|x$ 是 book 中的字母$\}$, $B=\{x|x$ 是 black 中的字母$\}$, 求 $A\cup B$, $A\cap B$。

(3) 给定自然数集合 N 的下列子集:

$$A=\{1, 2, 7, 8\},\ B=\{i|i^2<50\}$$
$$C=\{i|i \text{ 可被 3 整除}, 0\leqslant i\leqslant 30\}$$
$$D=\{i|i=2^k, k\in I_+, 0\leqslant k\leqslant 6\}$$

求下列集合:

a) $A\cup(B\cup(C\cup D))$

b) $A\cap(B\cap(C\cap D))$

c) $B-(A\cup C)$

d) $(\sim A\cap B)\cup D$

(4) 证明对所有集合 A、B 和 C，有

$$(A\cap B)\cup C=A\cap(B\cup C) \text{ iff } C\subseteq A$$

(5) 证明对任意集合 A、B、C，有

a) $(A-B)-C=A-(B\cup C)$

b) $(A-B)-C=(A-C)-B$

c) $(A-B)-C=(A-C)-(B-C)$

(6) 确定以下各式:

$\emptyset\cap\{\emptyset\}$, $\{\emptyset\}\cap\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}-\emptyset$, $\{\emptyset, \{\emptyset\}\}-\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}-\{\{\emptyset\}\}$

(7) 假定 A 和 B 是 E 的子集，证明以下各式中每个关系式彼此等价。

a) $A\subseteq B$, $\sim A\supseteq\sim B$, $A\cup B=B$, $A\cap B=A$

b) $A\cap B=\emptyset$, $A\subseteq\sim B$, $B\subseteq\sim A$

c) $A\cup B=E$, $\sim A\subseteq B$, $\sim B\subseteq A$

d) $A=B$, $A\oplus B=\emptyset$

(8) a) 已知 $A\cup B=A\cup C$，是否必须 $B=C$?

b) 已知 $A\cap B=A\cap C$，是否必须 $B=C$?

c) 已知 $A\oplus B=A\oplus C$，是否必须 $B=C$?

(9) 设 A、B、C 是集合，在什么条件下，下列命题是真的?

a) $(A-B)\cup(A-C)=A$

b) $(A-B)\cup(A-C)=\emptyset$

c) $(A-B)\cap(A-C)=\emptyset$

d) $(A-B)\oplus(A-C)=\emptyset$

(10) 借助于文氏图考察以下各命题的正确性:

a) 若 A、B 和 C 是 E 的子集，使得 $A\cap B\subseteq\sim C$ 和 $A\cup C\subseteq B$ 则 $A\cap C=\emptyset$

b) 若 A、B 和 C 是 E 的子集，使得 $A\subseteq\sim(B\cup C)$ 和 $B\subseteq\sim(A\cup C)$，则 $B=\emptyset$

(11) 证明:

a) $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$

b) $A\cup(B\oplus C)\neq(A\cup B)\oplus(A\cup C)$

*3-3 包含排斥原理

集合的运算，可用于有限个元素的计数问题。设 A_1, A_2 为有

限集合，其元素个数分别记为 $|A_1|$，$|A_2|$，根据集合运算的定义，显然以下各式成立。

$$|A_1\cup A_2|\leqslant|A_1|+|A_2|$$
$$|A_1\cap A_2|\leqslant\min(|A_1|,\ |A_2|)$$
$$|A_1-A_2|\geqslant|A_1|-|A_2|$$
$$|A_1\oplus A_2|=|A_1|+|A_2|-2|A_1\cap A_2|$$

这些公式可由图 3-3.1 的文氏图上直接得到说明。但是在有限集的元素计数问题中，下述定理有着更广泛的应用。

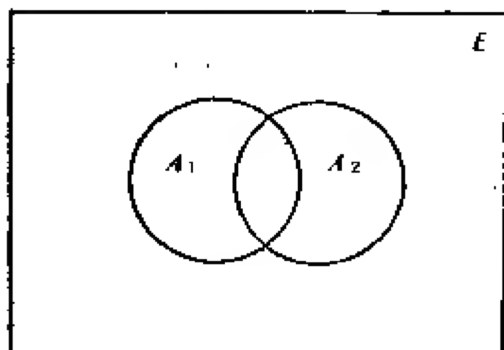


图 3-3.1

定理 3-3.1 设 A_1, A_2 为有限集合，其元素个数分别为 $|A_1|$，$|A_2|$，则

$$|A_1\cup A_2|=|A_1|+|A_2|-|A_1\cap A_2|$$

证明 a) 当 A_1 与 A_2 不相交，即 $A_1\cap A_2=\emptyset$，则

$$|A_1\cup A_2|=|A_1|+|A_2|$$

b) 若 $A_1\cap A_2\neq\emptyset$，则

$$|A_1|=|A_1\cap\sim A_2|+|A_1\cap A_2|$$
$$|A_2|=|\sim A_1\cap A_2|+|A_1\cap A_2|$$

所以 $|A_1|+|A_2|=|A_1\cap\sim A_2|+|\sim A_1\cap A_2|+2|A_1\cap A_2|$

但 $|A_1\cap\sim A_2|+|\sim A_1\cap A_2|+|A_1\cap A_2|=|A_1\cup A_2|$

故 $|A_1\cup A_2|=|A_1|+|A_2|-|A_1\cap A_2|$ □

这个定理，常称作包含排斥原理。

例题 1 假设在 10 名青年中有 5 名是工人，7 名是学生，其中兼具有工人与学生双重身份的青年有 3 名，问既不是工人又不是学生的青年有几名。

解 设工人的集合为 W，学生的集合为 S，则根据题设有：$|W|=5$，$|S|=7$，$|W\cap S|=3$。又因为 $|\sim W\cap\sim S|+|W\cup S|=10$，则

$$|\sim W\cap\sim S|=10-|W\cup S|=10-(|W|+|S|-|W\cap S|)$$
$$=10-(5+7-3)=1$$

所以既不是工人又不是学生的青年有一名。

对于任意三个集合 A_1, A_2 和 A_3, 我们可以推广定理 3-3.1 的结果为:

$$|A_1\cup A_2\cup A_3|=|A_1|+|A_2|+|A_3|-|A_1\cap A_2|-|A_1\cap A_3|-|A_2\cap A_3|+|A_1\cap A_2\cap A_3|$$

这个公式可以通过图 3-3.2 予以验证。

例题 2 在某工厂装配三十辆汽车,可供选择的设备是收音机,空气调节器和对讲机。已知其中 15 辆汽车有收音机,8 辆有空气调节器,6 辆有对讲机。而且其中 3 辆汽车这三样设备都有。我们希望知道至少有多少辆汽车没有提供任何设备。

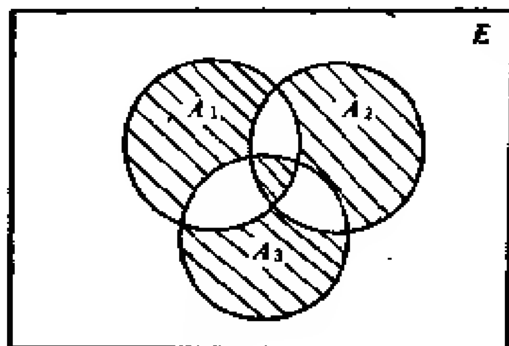


图 3-3.2

解 设 A_1, A_2, A_3 分别表示配有收音机、空气调节器和对讲机的汽车集合。因此

$$|A_1|=15,\ |A_2|=8,\ |A_3|=6$$

并且

$$|A_1\cap A_2\cap A_3|=3$$

故

$$\begin{aligned}|A_1\cup A_2\cup A_3|&=15+8+6-|A_1\cap A_2|-|A_1\cap A_3|-|A_2\cap A_3|+3\\&=32-|A_1\cap A_2|-|A_1\cap A_3|-|A_2\cap A_3|\end{aligned}$$

因为

$$|A_1\cap A_2|\geqslant|A_1\cap A_2\cap A_3|$$
$$|A_1\cap A_3|\geqslant|A_1\cap A_2\cap A_3|$$
$$|A_2\cap A_3|\geqslant|A_1\cap A_2\cap A_3|$$

我们得到

$$|A_1\cup A_2\cup A_3|\leqslant 32-3-3-3=23$$

即至多有 23 辆汽车有一个或几个供选择的设备,因此至少有 7 辆汽车不提供任何可选择的设备。

对于包含排斥原理,可以推广到 n 个集合的情况。

定理 3-3.2 设 A_1, A_2, …, A_n 为有限集合,其元素个数分别为 $|A_1|$, $|A_2|$, …, $|A_n|$, 则

$$\begin{aligned}|A_1\cup A_2\cup\cdots\cup A_n|=&\sum_{i=1}^{n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|\\&+\sum_{1\leqslant i<j<k\leqslant n}|A_i\cap A_j\cap A_k|\\&+\cdots+(-1)^{n-1}|A_1\cap A_2\cap A_3\cap\cdots\cap A_n|\quad(\text{I})\end{aligned}$$

证明　用归纳法证明。

(1) 归纳基础　$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

(2) 归纳步骤

设对于 $r-1$ 个集合等式成立。(归纳假设)

对于 r 个集合 $A_1, A_2, \cdots, A_{r-1}, A_r$, 由归纳基础可得

$$|A_1 \cup A_2 \cup \cdots \cup A_{r-1} \cup A_r| = |A_1 \cup A_2 \cup \cdots \cup A_{r-1}|$$
$$+ |A_r| - |A_r \cap (A_1 \cup A_2 \cup \cdots \cup A_{r-1})|$$
$$= |A_1 \cup A_2 \cup \cdots \cup A_{r-1}| + |A_r|$$
$$- |(A_r \cap A_1) \cup (A_r \cap A_2) \cup \cdots \cup (A_r \cap A_{r-1})| \quad \text{(II)}$$

对于 $r-1$ 个集合 $A_r \cap A_i (i=1, 2, \cdots, r-1)$, 由归纳假设

$$|(A_r \cap A_1) \cup (A_r \cap A_2) \cup \cdots \cup (A_r \cap A_{r-1})|$$
$$= \sum_{i=1}^{r-1} |A_r \cap A_i| - \sum_{1 \leq i < j \leq r-1} |(A_r \cap A_i) \cap (A_r \cap A_j)|$$
$$+ \cdots + (-1)^{r-2} |(A_r \cap A_1) \cap (A_r \cap A_2) \cap \cdots \cap (A_r \cap A_{r-1})|$$
$$= \sum_{i=1}^{r-1} |A_r \cap A_i| - \sum_{1 \leq i < j \leq r-1} |A_r \cap A_i \cap A_j|$$
$$+ \cdots + (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_{r-1} \cap A_r| \quad \text{(III)}$$

另外对 $r-1$ 个集合 $A_i (i=1, 2, \cdots, r-1)$, 由归纳假设有

$$|A_1 \cup A_2 \cup \cdots \cup A_{r-1}| = \sum_{i=1}^{r-1} |A_i| - \sum_{1 \leq i < j \leq r-1} |A_i \cap A_j|$$
$$+ \sum_{1 \leq i < j < k \leq r-1} |A_i \cap A_j \cap A_k|$$
$$+ \cdots + (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_{r-1}| \quad \text{(IV)}$$

将(III)、(IV)代入(II)得

$$|A_1 \cup A_2 \cup \cdots \cup A_r| = \sum_{i=1}^{r-1} |A_i| - \sum_{1 \leq i < j \leq r-1} |A_i \cap A_j|$$
$$+ \sum_{1 \leq i < j < k \leq r-1} |A_i \cap A_j \cap A_k|$$
$$+ \cdots + (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_{r-1}| + |A_r|$$
$$- \Big(\sum_{i=1}^{r-1} |A_r \cap A_i| - \sum_{1 \leq i < j \leq r-1} |A_r \cap A_i \cap A_j| + \cdots$$
$$+ (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_r| \Big)$$

整理后得

$$
\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_r| &= \sum_{i=1}^{r} |A_i| - \sum_{1 \le i < j \le r} |A_i \cap A_j| \\
&+ \sum_{1 \le i < j < k \le r} |A_i \cap A_j \cap A_k| \\
&+ \cdots + (-1)^{r-1} |A_1 \cap A_2 \cap \cdots \cap A_{r-1} \cap A_r|
\end{aligned}
$$

□

例题 3 求 1 到 250 之间能被 2, 3, 5 和 7 任何一个整除的整数个数。

解 设 A_1 表示 1 到 250 间能被 2 整除的整数集合，

A_2 表示 1 到 250 间能被 3 整除的整数集合，

A_3 表示 1 到 250 间能被 5 整除的整数集合，

A_4 表示 1 到 250 间能被 7 整除的整数集合，

$\lfloor x \rfloor$ 表示小于或等于 x 的最大整数。

$$|A_1| = \left\lfloor \frac{250}{2} \right\rfloor = 125 \qquad |A_2| = \left\lfloor \frac{250}{3} \right\rfloor = 83$$

$$|A_3| = \left\lfloor \frac{250}{5} \right\rfloor = 50 \qquad |A_4| = \left\lfloor \frac{250}{7} \right\rfloor = 35$$

$$|A_1 \cap A_2| = \left\lfloor \frac{250}{2 \times 3} \right\rfloor = 41 \qquad |A_1 \cap A_3| = \left\lfloor \frac{250}{2 \times 5} \right\rfloor = 25$$

$$|A_1 \cap A_4| = \left\lfloor \frac{250}{2 \times 7} \right\rfloor = 17 \qquad |A_2 \cap A_3| = \left\lfloor \frac{250}{3 \times 5} \right\rfloor = 16$$

$$|A_2 \cap A_4| = \left\lfloor \frac{250}{3 \times 7} \right\rfloor = 11 \qquad |A_3 \cap A_4| = \left\lfloor \frac{250}{5 \times 7} \right\rfloor = 7$$

$$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{250}{2 \times 3 \times 5} \right\rfloor = 8 \qquad |A_1 \cap A_2 \cap A_4| = \left\lfloor \frac{250}{2 \times 3 \times 7} \right\rfloor = 5$$

$$|A_1 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{2 \times 5 \times 7} \right\rfloor = 3 \qquad |A_2 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{3 \times 5 \times 7} \right\rfloor = 2$$

$$|A_1 \cap A_2 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{2 \times 3 \times 5 \times 7} \right\rfloor = 1$$

我们得到

$$
\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| &= 125 + 83 + 50 + 35 - 41 - 25 - 17 - 16 \\
&\quad - 11 - 7 + 8 + 5 + 3 + 2 - 1 = 193
\end{aligned}
$$

3-3 习题

(1) 设某校足球队有球衣 38 件，篮球队有球衣 15 件，棒球队有球衣 20 件，三队队员的总数为 58 人，且其中只有三人同时参加三队，试求同时参加二队的队员共有几人。

(2) 设由某项调查，发现学生阅读杂志的情况如下：

百分之六十阅读甲类杂志，
百分之五十阅读乙类杂志，
百分之五十阅读丙类杂志，
百分之三十阅读甲类杂志与乙类杂志，
百分之三十阅读乙类杂志与丙类杂志，
百分之三十阅读甲类杂志与丙类杂志，
百分之十阅读三类杂志。

问 a) 试求确实阅读两类杂志的学生百分比？

b) 试求不读任何杂志的学生的百分比？

(3) 75 个儿童到公园游乐场，他们在那里可以骑旋转木马，坐滑行铁道，乘宇宙飞船，已知其中 20 人这三种东西都乘坐过，其中 55 人至少乘坐过其中的两种。若每样乘坐一次的费用是 0.50 元，公园游乐场总共收入 70 元，试确定有多少儿童没有乘过其中任何一种。

(4) a) 在一个班级的 50 个学生中，有 26 人在第一次考试中得到 A，21 人在第二次考试中得到 A，假如有 17 人两次考试都没有得到 A，问有多少学生两次考试中都得到 A。

b) 在这些学生中，如果第一次考试中得到 A 的人数等于第二次考试中得到 A 的人数，如果仅仅在一次考试中得到 A 的学生总数是 40，并且如果有 4 个学生两次考试都没有得到 A，问有多少学生仅在第一次考试中取得 A？问有多少学生仅在第二次考试中取得 A？又问有多少学生在两次考试中都得 A？

(5) 对 200 名大学一年级的学生进行调查的结果是：其中 67 人学数学，47 人学物理，95 人学生物，26 人既学数学又学生物，28 人既学数学又学物理，27 人既学物理又学生物，50 人这三门课都不学。

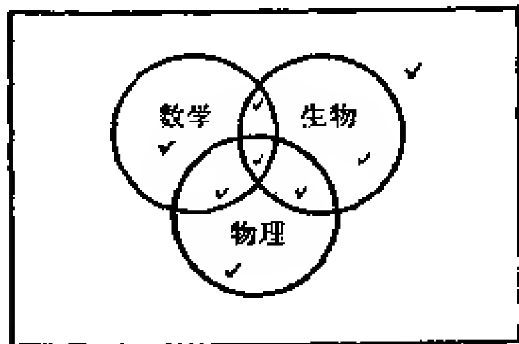


图 3-3.3

a) 求出对三门课都学的学生人数，

b) 在文氏图(图 3-3.3) 中以正确的学生人数填入其中 8 个区域。

3-4 序偶与笛卡尔积

在日常生活中，有许多事物是成对出现的，而且这种成对出现的事物，具有一定的顺序。例如，上、下；左、右；$3<4$；张华高于李

明；中国地处亚洲；平面上点的坐标等。一般地说，两个具有固定次序的客体组成一个序偶，它常常表达两个客体之间的关系。记作 $\langle x, y\rangle$。上述各例可分别表示为〈上、下〉；〈左、右〉；$\langle 3, 4\rangle$；〈张华、李明〉；〈中国，亚洲〉；$\langle a, b\rangle$ 等。

序偶可以看作是具有两个元素的集合[注]。但它与一般集合不同的是序偶具有确定的次序。在集合中 $\{a, b\}=\{b, a\}$，但对序偶 $\langle a, b\rangle\neq\langle b, a\rangle$。

定义 3-4.1 两个序偶相等，$\langle x, y\rangle=\langle u, v\rangle$，iff $x=u$，$y=v$。

应该指出，序偶 $\langle a, b\rangle$ 中两个元素不一定来自同一个集合，它们可以代表不同类型的事物。例如，a 代表操作码，b 代表地址码，则序偶 $\langle a, b\rangle$ 就代表一条单地址指令；当然亦可将 a 代表地址码，b 代表操作码，$\langle a, b\rangle$ 仍代表一条单地址指令；但上述这种约定，一经确定，序偶的次序就不能再予以变化了。在序偶 $\langle a, b\rangle$ 中，a 称第一元素，b 称第二元素。

序偶的概念可以推广到三元组的情况。

三元组是一个序偶，其第一元素本身也是一个序偶，可形式化表示为 $\langle\langle x, y\rangle, z\rangle$。由序偶相等的定义，可以知道 $\langle\langle x, y\rangle, z\rangle=\langle\langle u, v\rangle, w\rangle$，iff $\langle x, y\rangle=\langle u, v\rangle$，$z=w$，即 $x=u$，$y=v$，$z=w$。今后约定三元组可记作 $\langle x, y, z\rangle$。应该注意的是：当 $x\neq y$ 时，$\langle x, y, z\rangle\neq\langle y, x, z\rangle$。$\langle\langle x, y\rangle, z\rangle\neq\langle x, \langle y, z\rangle\rangle$，因为 $\langle x, \langle y, z\rangle\rangle$ 不是三元组。同理四元组被定义为一个序偶，其第一元素为三元组，故四元组有形式为 $\langle\langle x, y, z\rangle, w\rangle$ 且

$$\langle\langle x, y, z\rangle, w\rangle=\langle\langle p, q, r\rangle, s\rangle$$
$$\Leftrightarrow(x=p)\wedge(y=q)\wedge(z=r)\wedge(w=s)$$

这样，n 元组可写为 $\langle\langle x_1, x_2, \cdots, x_{n-1}\rangle, x_n\rangle$ 且

$$\langle\langle x_1, x_2, \cdots, x_{n-1}\rangle, x_n\rangle=\langle\langle y_1, y_2, \cdots, y_{n-1}\rangle, y_n\rangle$$
$$\Leftrightarrow(x_1=y_1)\wedge(x_2=y_2)\wedge\cdots\wedge(x_{n-1}=y_{n-1})\wedge(x_n=y_n)$$

一般地，n 元组可简写为 $\langle x_1, x_2, \cdots, x_n\rangle$，第 i 个元素 x_i 称作 n 元

[注] 可以定义 $\langle x, y\rangle:=\{\{x\}, \{x, y\}\}$ 见 R·R·Stoll 著《Set Theory and Logic》p. 24。

组的第 i 个坐标。

序偶 $\langle x, y\rangle$ 其元素可以分别属于不同的集合，因此任给两个集合 A 和 B，我们可以定义一种序偶的集合。

定义 3-4.2 令 A 和 B 是任意两个集合，若序偶的第一个成员是 A 的元素，第二个成员是 B 的元素，所有这样的序偶集合，称为集合 A 和 B 的笛卡尔乘积或直积。记作 $A\times B$。

$$A\times B=\{\langle x, y\rangle \mid (x\in A)\wedge(y\in B)\}$$

例题 1 若 $A=\{\alpha, \beta\}$，$B=\{1, 2, 3\}$，求 $A\times B$，$B\times A$，$A\times A$，$B\times B$，以及 $(A\times B)\cap(B\times A)$。

解

$$A\times B=\{\langle\alpha, 1\rangle, \langle\alpha, 2\rangle, \langle\alpha, 3\rangle, \langle\beta, 1\rangle, \langle\beta, 2\rangle, \langle\beta, 3\rangle\}$$

$$B\times A=\{\langle 1, \alpha\rangle, \langle 1, \beta\rangle, \langle 2, \alpha\rangle, \langle 2, \beta\rangle, \langle 3, \alpha\rangle, \langle 3, \beta\rangle\}$$

$$A\times A=\{\langle\alpha, \alpha\rangle, \langle\alpha, \beta\rangle, \langle\beta, \alpha\rangle, \langle\beta, \beta\rangle\}$$

$$B\times B=\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$$

$$(A\times B)\cap(B\times A)=\emptyset$$

由例题 1 可以看出 $A\times B\neq B\times A$。

我们约定若 $A=\emptyset$ 或 $B=\emptyset$，则 $A\times B=\emptyset$。

由笛卡尔积定义可知：

$$\begin{aligned}(A\times B)\times C&=\{\langle\langle a, b\rangle, c\rangle \mid (\langle a, b\rangle\in A\times B)\wedge(c\in C)\}\\&=\{\langle a, b, c\rangle \mid (a\in A)\wedge(b\in B)\wedge(c\in C)\}\end{aligned}$$

$$A\times(B\times C)=\{\langle a, \langle b, c\rangle\rangle \mid (a\in A)\wedge(\langle b, c\rangle\in B\times C)\}$$

由于 $\langle a, \langle b, c\rangle\rangle$ 不是三元组，所以

$$(A\times B)\times C\neq A\times(B\times C)$$

定理 3-4.1 设 A，B，C 为任意三个集合，则有

a) $A\times(B\cup C)=(A\times B)\cup(A\times C)$

b) $A\times(B\cap C)=(A\times B)\cap(A\times C)$

c) $(A\cup B)\times C=(A\times C)\cup(B\times C)$

d) $(A\cap B)\times C=(A\times C)\cap(B\times C)$

证明 a) 设 $\langle x, y\rangle\in A\times(B\cup C)$，则 $x\in A$，$y\in(B\cup C)$，即 $x\in A$ 且 $(y\in B$ 或 $y\in C)$。

故　　$(x\in A,\ y\in B)$　或　$(x\in A,\ y\in C)$

得到　　$\langle x,\ y\rangle\in A\times B$

或　　$\langle x,\ y\rangle\in A\times C$, $\langle x,\ y\rangle\in[(A\times B)\cup(A\times C)]$

所以　　$A\times(B\cup C)\subseteq(A\times B)\cup(A\times C)$

又设　　$\langle x,\ y\rangle\in[(A\times B)\cup(A\times C)]$

则　　$\langle x,\ y\rangle\in A\times B$

或 $\langle x,\ y\rangle\in A\times C$，即 $x\in A$，$y\in B$ 或 $x\in A$，$y\in C$，即 $x\in A$ 且($y\in B$ 或 $y\in C$)。

故　　$x\in A$ 且 $y\in(B\cup C)$

得到　　$\langle x,\ y\rangle\in A\times(B\cup C)$

所以　　$(A\times B)\cup(A\times C)\subseteq A\times(B\cup C)$

因此　　$A\times(B\cup C)=(A\times B)\cup(A\times C)$

c) 若 $\langle x,\ y\rangle\in(A\cup B)\times C\Leftrightarrow(x\in(A\cup B)\wedge y\in C)$

$$\Leftrightarrow(x\in A\vee x\in B)\wedge(y\in C)$$

$$\Leftrightarrow(x\in A\wedge y\in C)\vee(x\in B\wedge y\in C)$$

$$\Leftrightarrow(\langle x,\ y\rangle\in A\times C)\vee(\langle x,\ y\rangle\in B\times C)$$

$$\Leftrightarrow\langle x,\ y\rangle\in((A\times C)\cup(B\times C))$$

因此　　$(A\cup B)\times C=(A\times C)\cup(B\times C)$　□

定理3-4.2　若 $C\neq\emptyset$，则

$$A\subseteq B\Leftrightarrow(A\times C\subseteq B\times C)\Leftrightarrow(C\times A\subseteq C\times B)$$

证明　若 $y\in C$，假定 $A\subseteq B$，有

$$\langle x,\ y\rangle\in A\times C\Rightarrow(x\in A\wedge y\in C)\Rightarrow(x\in B\wedge y\in C)$$

$$\Rightarrow\langle x,y\rangle\in B\times C$$

因此　　$A\times C\subseteq B\times C$

反之，若 $C\neq\emptyset$，$A\times C\subseteq B\times C$，取 $y\in C$，则有

$$x\in A\Rightarrow(x\in A)\wedge(y\in C)$$

$$\Leftrightarrow(\langle x,\ y\rangle\in A\times C)$$

$$\Rightarrow(\langle x,\ y\rangle\in B\times C)$$

$$\Leftrightarrow(x\in B)\wedge(y\in C)$$

$$\Rightarrow x\in B$$

因此 $$A \subseteq B$$

同样，定理的第二部分 $A \subseteq B \Leftrightarrow (C \times A \subseteq C \times B)$ 可以类似地证明。 □

定理 3-4.3 设 A、B、C、D 为四个非空集合，则 $A \times B \subseteq C \times D$ 的充要条件为 $A \subseteq C$，$B \subseteq D$。

证明 若 $A \times B \subseteq C \times D$，对任意 $x \in A$ 和 $y \in B$ 有

$$\begin{aligned}(x \in A) \wedge (y \in B) &\Rightarrow (\langle x, y\rangle \in A \times B)\\ &\Rightarrow (\langle x, y\rangle \in C \times D)\\ &\Rightarrow (x \in C) \wedge (y \in D)\end{aligned}$$

即 $A \subseteq C$ 且 $B \subseteq D$。

反之，若 $A \subseteq C$ 且 $B \subseteq D$，设任意 $x \in A$ 和 $y \in B$，我们有

$$\begin{aligned}\langle x, y\rangle \in A \times B &\Leftrightarrow (x \in A \wedge y \in B) \Rightarrow (x \in C \wedge y \in D)\\ &\Leftrightarrow (\langle x, y\rangle \in C \times D)\end{aligned}$$

因此 $A \times B \subseteq C \times D$ □

因为两集合的笛卡尔积仍是一个集合，故对于有限集合可以进行多次的笛卡尔积运算。

为了与 n 元组一致，我们约定：

$$A_1 \times A_2 \times A_3 = (A_1 \times A_2) \times A_3$$

$$\begin{aligned}A_1 \times A_2 \times A_3 \times A_4 &= (A_1 \times A_2 \times A_3) \times A_4\\ &= ((A_1 \times A_2) \times A_3) \times A_4\end{aligned}$$

一般地，
$$\begin{aligned}A_1 \times A_2 \times \cdots \times A_n &= (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n\\ &= \{\langle x_1, x_2, \cdots, x_n\rangle \mid (x_1 \in A_1) \wedge (x_2 \in A_2) \wedge \cdots \wedge (x_n \in A_n)\}\end{aligned}$$

故 $A_1 \times A_2 \times \cdots \times A_n$ 是有关 n 元组构成的集合。特别地，$A \times A$ 可以写成 A^2，同样地 $A \times A \times A = A^3$，$\cdots$，$\overbrace{A \times A \times \cdots \times A}^{n} = A^n$。

3-4 习题

(1) 设 $A = \{0, 1\}$，$B = \{1, 2\}$，确定下面集合。

a) $A \times \{1\} \times B$

b) $A^2 \times B$

c) $(B \times A)^2$

(2) 设 $A=\{a, b\}$，构成集合 $\mathscr{P}(A) \times A$。

(3) 下列各式中哪些成立？哪些不成立？为什么？

a) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$

b) $(A - B) \times (C - D) = (A \times C) - (B \times D)$

c) $(A \oplus B) \times (C \oplus D) = (A \times C) \oplus (B \times D)$

d) $(A - B) \times C = (A \times C) - (B \times C)$

e) $(A \oplus B) \times C = (A \times C) \oplus (B \times C)$

(4) 证明：若 $X \times X = Y \times Y$，则 $X = Y$。

(5) 证明：若 $X \times Y = X \times Z$，且 $X \neq \emptyset$，则 $Y = Z$。

3-5 关系及其表示

关系是一个基本概念，在日常生活中我们都熟悉关系这词的含义，例如兄弟关系；上下级关系；位置关系等。在数学上关系可表达集合中元素间的联系。如“3 小于 5”；“x 大于 y”；“点 a 在 b 与 c 之间”等。我们又知道，序偶可以表达两个客体、三个客体或 n 个客体之间的联系，因此用序偶表达关系这个概念是非常自然的，下面先以实例说明。

例如，电影票与座位之间有对号关系。设 X 表示电影票的集合，Y 表示座位的集合，则对于任意的 $x \in X$ 和 $y \in Y$，必有 x 与 y 有“对号”关系和 x 与 y 没有“对号”关系两种情况的一种，令 R 表示“对号”关系，则上述问题可表达为 xRy 或 $x\not R y$，亦可记为 $\langle x, y\rangle \in R$ 或 $\langle x, y\rangle \notin R$，因此我们看到对号关系 R 是序偶的集合。

定义 3-5.1 任一序偶的集合确定了一个二元关系 R，R 中任一序偶 $\langle x, y\rangle$ 可记作 $\langle x, y\rangle \in R$ 或 xRy。不在 R 中的任一序偶 $\langle x, y\rangle$ 可记作 $\langle x, y\rangle \notin R$ 或 $x\not R y$。

例如，在实数中关系 $>$ 可记作 $> = \{\langle x, y\rangle \mid x, y \text{ 是实数且 } x>y\}$。

定义 3-5.2 令 R 为二元关系，由 $\langle x, y\rangle \in R$ 的所有 x 组成的集合 $\mathrm{dom}R$ 称为 R 的前域，即

$$\mathrm{dom}\, R = \{x \mid (\exists y)(\langle x, y\rangle \in R)\}$$

使 $\langle x, y\rangle \in R$ 的所有 y 组成的集合 $\mathrm{ran}R$ 称作 R 的值域，即

$$\mathrm{ran}\, R = \{y \mid (\exists x)(\langle x, y\rangle \in R)\}$$

R 的前域和值域一起称作 R 的域，记作 FLD R，即

$$\mathrm{FLD}\, R = \mathrm{dom}\, R \cup \mathrm{ran}\, R$$

例题 1 设 $A = \{1, 2, 3, 5\}$，$B = \{1, 2, 4\}$，

$$H = \{\langle 1, 2\rangle, \langle 1, 4\rangle, \langle 2, 4\rangle, \langle 3, 4\rangle\},$$

求 dom H，ran H，FLD H。

解　$\mathrm{dom}\, H = \{1, 2, 3\}$，$\mathrm{ran}\, H = \{2, 4\}$，$\mathrm{FLD}\, H = \{1, 2, 3, 4\}$。

由于关系是序偶的集合，如果序偶的第一元素和第二元素分别属于不同的集合，那么关系就是两集合直积的子集。

定义 3-5.3 令 X 和 Y 是任意两个集合，直积 $X \times Y$ 的子集 R 称作 X 到 Y 的关系。

X 到 Y 的关系 R，可以图 3-5.1 所示。

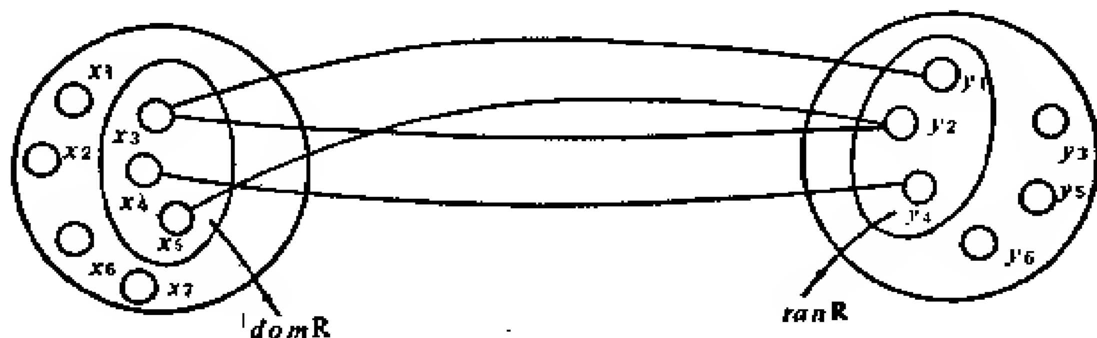


图 3-5.1

从关系的定义可以看到 $\mathrm{dom}\, R \subseteq X$，$\mathrm{ran}\, R \subseteq Y$，由例题 1 表明 $H \subseteq A \times B$，$\mathrm{dom}\, H \subseteq A$，$\mathrm{ran}\, H \subseteq B$，$\mathrm{FLD}\, H = \mathrm{dom}\, H \cup \mathrm{ran}\, H \subseteq A \cup B$。

我们今后把 $X \times Y$ 的两个平凡子集 $X \times Y$ 和 $\emptyset$，分别称为 X 到 Y 的全域关系和空关系。

当 $X = Y$ 时，关系 R 是 $X \times X$ 的子集，这时称 R 为在 X 上的二元关系。

例题 2 设 $X=\{1, 2, 3, 4\}$，求 X 上的关系 $>$ 及 $\mathrm{dom}>$，$\mathrm{ran}>$。

解 $>=\{\langle 2, 1\rangle, \langle 3, 1\rangle, \langle 4, 1\rangle, \langle 3, 2\rangle, \langle 4, 2\rangle, \langle 4, 3\rangle\}$

$\mathrm{dom}>=\{2, 3, 4\}$，$\mathrm{ran}>=\{1, 2, 3\}$。

例题 3 若 $H=\{f, m, s, d\}$ 表示一个家庭中父、母、子、女四个人的集合，确定 H 上的全域关系和空关系，另外再确定 H 上的一个关系，指出该关系的值域和前域。

解 设 H 上的同一家庭成员的关系为 H_1，

$$
\begin{aligned}
H_1=\{&\langle f, m\rangle, \langle f, s\rangle, \langle f, d\rangle, \langle m, f\rangle, \langle m, s\rangle, \langle m, d\rangle,\\
&\langle s, f\rangle, \langle s, m\rangle, \langle s, d\rangle, \langle d, f\rangle, \langle d, m\rangle, \langle d, s\rangle,\\
&\langle f, f\rangle, \langle m, m\rangle, \langle s, s\rangle, \langle d, d\rangle\}
\end{aligned}
$$

设 H 上的互不相识的关系为 H_2，$H_2=\emptyset$，则 H_1 为全域关系，H_2 为空关系。

设 H 上的长幼关系为 H_3，

$$H_3=\{\langle f, s\rangle, \langle f, d\rangle, \langle m, s\rangle, \langle m, d\rangle\}$$

$\mathrm{dom}H_3=\{f, m\}$，$\mathrm{ran}H_3=\{s, d\}$。

定义 3-5.4 设 I_X 是 X 上的二元关系且满足 $I_X=\{\langle x, x\rangle \mid x\in X\}$，则称 I_X 是 X 上的恒等关系。

例如，$A=\{1, 2, 3\}$，则 $I_A=\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$。

因为关系是序偶的集合，故同一域上的关系，可以进行集合的所有运算。

例题 4 设 $X=\{1, 2, 3, 4\}$，若 $H=\left\{\langle x, y\rangle \,\middle|\, \frac{x-y}{2}\text{ 是整数}\right\}$，$S=\left\{\langle x, y\rangle \,\middle|\, \frac{x-y}{3}\text{ 是正整数}\right\}$，求 $H\cup S$，$H\cap S$，$\sim H$，$S-H$。

解

$$
\begin{aligned}
H=\{&\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle,\\
&\langle 3, 1\rangle, \langle 4, 4\rangle, \langle 4, 2\rangle\}
\end{aligned}
$$

$$S=\{\langle 4, 1\rangle\}$$

$$
\begin{aligned}
H\cup S=\{&\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle, \langle 3, 1\rangle,\\
&\langle 4, 4\rangle, \langle 4, 2\rangle, \langle 4, 1\rangle\}
\end{aligned}
$$

$$H\cap S=\emptyset$$

$$
\begin{aligned}
\sim H=\{&\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle,\\
&\langle 1, 4\rangle, \langle 4, 1\rangle\}
\end{aligned}
$$

$$S-H=\{\langle 4, 1\rangle\}$$

定理 3-5.1 若 Z 和 S 是从集合 X 到集合 Y 的两个关系，

则 Z、S 的并、交、补、差仍是 X 到 Y 的关系。

证明　因为 $Z \subseteq X \times Y$, $S \subseteq X \times Y$

故
$$Z \cup S \subseteq X \times Y,\ Z \cap S \subseteq X \times Y$$
$$\sim S = (X \times Y - S) \subseteq X \times Y$$
$$Z - S = Z \cap \sim S \subseteq X \times Y$$
□

从上面我们可以知道，X 到 Y 的关系 R 是 $X \times Y$ 的子集，如果令 X 和 Y 为有限集，则二元关系 R 除了可用序偶集合的形式表达以外，亦可用矩阵或图形表示。

设给定两个有限集合 $X=\{x_1, x_2, \cdots, x_m\}$，$Y=\{y_1, y_2, \cdots, y_n\}$，$R$ 为从 X 到 Y 的一个二元关系。则对应于关系 R 有一个关系矩阵 $M_R=[r_{ij}]_{m\times n}$，其中

$$r_{ij}=\begin{cases}1 & 当\ \langle x_i, y_j\rangle \in R \\ 0 & 当\ \langle x_i, y_j\rangle \notin R\end{cases}$$
$$(i=1, 2, \cdots, m;\ j=1, 2, \cdots, n)$$

例题 5　设 $X=\{x_1, x_2, x_3, x_4\}$，$y=\{y_1, y_2, y_3\}$，
$R=\{\langle x_1, y_1\rangle, \langle x_1, y_3\rangle, \langle x_2, y_2\rangle, \langle x_2, y_3\rangle, \langle x_3, y_1\rangle, \langle x_4, y_1\rangle, \langle x_4, y_2\rangle\}$，写出关系矩阵 M_R。

解
$$M_R=\begin{bmatrix}1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0\end{bmatrix}$$

例题 6　设 $A=\{1, 2, 3, 4\}$，写出集合 A 上大于关系 $>$ 的关系矩阵。

解　$>=\{\langle 2, 1\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle, \langle 4, 1\rangle, \langle 4, 2\rangle, \langle 4, 3\rangle\}$

故
$$M_>=\begin{bmatrix}0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0\end{bmatrix}$$

有限集的二元关系亦可用图形来表示，设集合 $X=\{x_1, x_2, \cdots, x_m\}$ 到 $Y=\{y_1, y_2, \cdots, y_n\}$ 上的一个二元关系为 R，首先我们在平面上作出 m 个结点分别记作 $x_1, x_2, \cdots, x_m$，然后另外作 n 个结点分别记作 $y_1, y_2, \cdots, y_n$。如果 $x_i R y_j$，则可自结点 x_i 至结

点 y_j 处作一有向弧，其箭头指向 y_j，如果 $x_i \not R y_j$，则 x_i 与 y_j 间没有线段联结。这种方法联结起来的图就称为 R 的关系图。

例题 7 画出例题 5 的关系图。

解 例题 5 的关系图如图 3-5.2 所示：

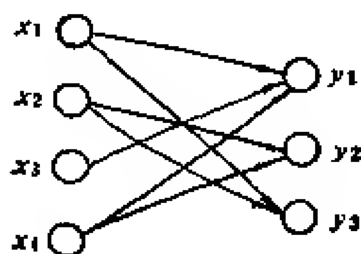


图 3-5.2

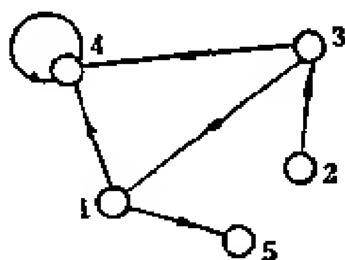


图 3-5.3

例题 8 设 $A=\{1, 2, 3, 4, 5\}$，在 A 上的二元关系 R 给定为：$R=\{\langle 1, 5\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 4\rangle, \langle 4, 4\rangle\}$ 画出 R 的关系图。

解 因为 R 是 A 上的关系，故只需画出 A 中的每个元素即可。如果 a_iRa_j，就画一条由 a_i 到 a_j 的有向弧，本题的关系图如图 3-5.3 所示。

由于关系图主要表达结点与结点之间的邻接关系，故关系图中对结点位置和线段的长短无关，本例的关系 R 亦可表达为如图 3-5.4 所示。

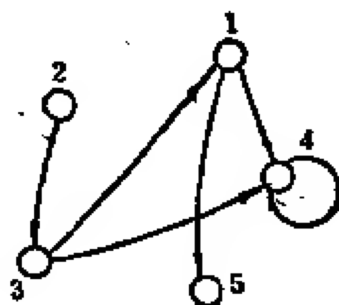


图 3-5.4

我们需要指出，从 X 到 Y 的关系 R 是 $X\times Y$ 的子集，即 $R\subseteq X\times Y$，而 $X\times Y\subseteq (X\cup Y)\times(X\cup Y)$，所以 $R\subseteq (X\cup Y)\times(X\cup Y)$。令 $Z=X\cup Y$，则 $R\subseteq Z\times Z$，因此，我们今后通常限于讨论同一集合上的关系。

3-5 习题

(1) 列出所有从 $X=\{a, b, c\}$ 到 $Y=\{S\}$ 的关系。

(2) 在一个有 n 个元素的集合上，可以有多少种不同的关系。

(3) 设 $A=\{6:00, 6:30, 7:00, \cdots, 9:30, 10:00\}$ 表示在晚上每隔半小时的九个时刻的集合，设 $B=\{3, 12, 15, 17\}$ 表示本地四个电视频道的集合，设 R_1 和 R_2 是从 A 到 B 的两个二元关系。对于二元关系 R_1，R_2，

$R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 \oplus R_2$ 和 $R_1 - R_2$ 分别可以得出怎样的解释。

(4) 设 L 表示关系"小于或等于", D 表示整除, L 和 D 均定义于 $\{1, 2, 3, 6\}$, 分别写出 L 和 D 的所有元素,并求出 $L \cap D$。

(5) 对下列每一式所给出 A 上的二元关系,试给出关系图。

a) $\{\langle x, y\rangle \mid 0 \leqslant x \wedge y \leqslant 3\}$, $A = \{0, 1, 2, 3, 4\}$

b) $\{\langle x, y\rangle \mid 2 \leqslant x, y \leqslant 7 \wedge x$ 除尽 $y\}$, 这里 $A = \{n \mid n \in N \wedge n \leqslant 10\}$

c) $\{\langle x, y\rangle \mid 0 \leqslant x - y < 3\}$, 这里 $A = \{0, 1, 2, 3, 4\}$

d) $\{\langle x, y\rangle \mid x$ 和 y 是互质的$\}$, 这里 $A = \{2, 3, 4, 5, 6\}$

(6) 对 $\{0, 1, 2, 3, 4, 5, 6\}$ 上的二元关系, $\{\langle x, y\rangle \mid x < y \vee x$ 是质数$\}$, 写出关系矩阵。

(7) 设 $P = \{\langle 1, 2\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle\}$ 和 $Q = \{\langle 1, 3\rangle, \langle 2, 4\rangle, \langle 4, 2\rangle\}$ 找出 $P \cup Q$, $P \cap Q$, $\operatorname{dom} P$, $\operatorname{dom} Q$, $\operatorname{ran} P$, $\operatorname{ran} Q$, $\operatorname{dom}(P \cap Q)$, $\operatorname{ran}(P \cap Q)$

(8) 证明集合 A 是一个关系,当且仅当 $A \subseteq \operatorname{dom} A \times \operatorname{ran} A$。

3-6 关系的性质

有了表达关系的各种方法,下面就可以对关系作进一步的讨论。我们特别注意的是在集合 X 上的二元关系 R 的一些特殊性质。

定义 3-6.1 设 R 为定义在集合 X 上的二元关系,如果对于每个 $x \in X$, 有 xRx, 则称二元关系 R 是自反的。

$$R \text{ 在 } X \text{ 上自反} \Leftrightarrow (\forall x)(x \in X \rightarrow xRx)$$

例如,在实数集合中,"$\leqslant$"是自反的,因为对于任意实数 $x \leqslant x$ 成立。又如平面上三角形的全等关系是自反的。

定义 3-6.2 设 R 为定义在集合 X 上的二元关系,如果对于每个 $x, y \in X$, 每当 xRy, 就有 yRx, 则称集合 X 上关系 R 是对称的。

$$R \text{ 在 } X \text{ 上对称} \Leftrightarrow (\forall x)(\forall y)(x \in X \wedge y \in X \wedge xRy \rightarrow yRx)$$

例如,平面上诸三角形集合中三角形的相似关系是对称的,因为若三角形 A 相似三角形 B, 则三角形 B 必相似三角形 A。同理,在同一街道居住的邻居关系也是对称的。有些集合 X 上的关系,既是自反的,又是对称的。

例题 1 设 $A=\{2, 3, 5, 7\}$，$R=\left\{\langle x, y\rangle \middle| \frac{x-y}{2}\text{是整数}\right\}$，验证 R 在 A 上是自反和对称的。

证 因为对于任意 $x\in A$，$\frac{x-x}{2}=0$，即 $\langle x, x\rangle\in R$，故 R 是自反的。

又设 $x, y\in A$，如果 $\langle x, y\rangle\in R$，即 $\frac{x-y}{2}$ 是整数，则 $\frac{y-x}{2}$ 也必是整数，即 $\langle y, x\rangle\in R$，因此 R 是对称的。

定义 3-6.3 设 R 为定义在集合 X 上的二元关系，如果对于任意 $x, y, z\in X$，每当 xRy，yRz 时就有 xRz，称关系 R 在 X 上是传递的。

R 在 X 上传递

$$\Leftrightarrow(\forall x)(\forall y)(\forall z)(x\in X\wedge y\in X\wedge z\in X\wedge xRy\wedge yRz\rightarrow xRz)$$

例如，在实数集合中关系 $\leqslant$、$<$ 和 $=$，都是传递的。又如，设 A 是人的集合，R 是 A 上的二元关系，若 $\langle a, b\rangle\in R$ 当且仅当 a 是 b 的祖先，显然祖先关系 R 是传递的。

例题 2 设 $X=\{1, 2, 3\}$，$R_1=\{\langle 1, 2\rangle, \langle 2, 2\rangle\}$，$R_2=\{\langle 1, 2\rangle\}$，$R_3=\{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle\}$，$R_1$，$R_2$ 和 R_3 都是传递关系吗？

解 根据传递的定义，R_1 和 R_2 是传递的。但对于 R_3，因为 $\langle 1, 2\rangle\in R_3$，$\langle 2, 1\rangle\in R_3$，但 $\langle 1, 1\rangle\notin R_3$，$\langle 2, 2\rangle\notin R_3$，故 R_3 不是传递的。

定义 3-6.4 设 R 为定义在集合 X 上的二元关系，如果对于每一个 $x\in X$，都有 $\langle x, x\rangle\notin R$，则 R 称作反自反的。

R 在 X 上反自反 $\Leftrightarrow(\forall x)(x\in X\rightarrow\langle x, x\rangle\notin R)$

例如，数的大于关系，日常生活中的父子关系等都是反自反的。应该注意：一个不是自反的关系，不一定就是反自反的。

例题 3 $A=\{1, 2, 3\}$，$S=\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 3, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$，验证 S 不是自反也不是反自反的。

证明 因为 $2\in A$，但 $\langle 2, 2\rangle\notin S$，故 S 不是自反的，又 $1\in A$，$3\in A$ 但 $\langle 1,1\rangle\in S$，$\langle 3, 3\rangle\in S$，故 S 也不是反自反的。

定义 3-6.5 设 R 为定义在集合 X 上的二元关系，对于每一个 $x, y\in X$，每当 xRy 和 yRx 必有 $x=y$，则称 R 在 X 上是反对

称的，即是

$$(\forall x)(\forall y)(x\in X\wedge y\in X\wedge xRy\wedge yRx\rightarrow x=y)$$

例如实数集合中 $\leqslant$ 是反对称的，集合的 $\subseteq$ 关系是反对称的。因为

$$\begin{aligned}(xRy)\wedge(yRx)\rightarrow(x=y)&\Leftrightarrow\urcorner(x=y)\rightarrow\urcorner((xRy)\wedge(yRx))\\&\Leftrightarrow\urcorner(x=y)\rightarrow(x\not R y)\vee(y\not R x)\\&\Leftrightarrow(x=y)\vee(x\not R y)\vee(y\not R x)\\&\Leftrightarrow\urcorner((x\neq y)\wedge(xRy))\vee(y\not R x)\\&\Leftrightarrow(x\neq y)\wedge(xRy)\rightarrow y\not R x\end{aligned}$$

故关系 R 的反对称的定义亦可表示为

$$(\forall x)(\forall y)(x\in X\wedge y\in X\wedge x\neq y\wedge xRy\rightarrow y\not R x)$$

注意：可能有某种关系，既是对称的，又是反对称的。

例如，$A=\{1, 2, 3\}$，$S=\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$，则 S 在 A 上是对称的也是反对称的。但如，$A=\{a, b, c\}$，$N=\{\langle a, b\rangle, \langle a, c\rangle, \langle c, a\rangle\}$，则 N 既不是对称关系，又不是反对称关系。

例题 4 设某人有三个儿子，组成集合 $A=\{T, G, H\}$，在 A 上的兄弟关系具有哪些性质。

解 在 A 上的兄弟关系是反自反的和对称的。

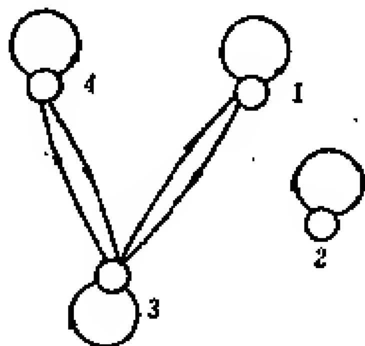


图 3-6.1

注意：兄弟关系并不具有传递性，这是因为若 TRG，根据对称必有 GRT，但 $\langle T, T\rangle\notin R$，故 R 不是传递的。

例题 5 集合 $I=\{1, 2, 3, 4\}$，I 上的关系 $R=\{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 3, 1\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle, \langle 4, 4\rangle\}$ 讨论 R 的性质。

解 写出 R 的关系矩阵并画出关系图如图 3-6.1 所示。关系矩阵

$$\begin{bmatrix}1&0&1&0\\0&1&0&0\\1&0&1&1\\0&0&1&1\end{bmatrix}$$

从例题 5 的关系矩阵和关系图容易看出，R 是自反的，对称的。一般地说：

(1) 若关系 R 是自反的，当且仅当在关系矩阵中，对角线上的所有元素都是1，在关系图上每个结点都有自回路。

(2) 若关系 R 是对称的，当且仅当关系矩阵是对称的，且在关系图上，任两个结点间若有定向弧线，必是成对出现的。

(3) 若关系 R 是反自反的，当且仅当关系矩阵对角线的元素皆为零，关系图上每个结点都没有自回路。

(4) 若关系 R 是反对称的，当且仅当关系矩阵中以主对角线对称的元素不能同时为1，在关系图上两个不同结点间的定向弧线不可能成对出现。

传递的特征较复杂，不易从关系矩阵和关系图中直接判断。

3-6 习题

(1) 分析集合 $A=\{1, 2, 3\}$ 上的下述五个关系。

$R=\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 3, 3\rangle\}$

$S=\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$

$T=\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle\}$

$\emptyset=$空关系

$A\times A=$全域关系

判断 A 中的上述关系是不是 a) 自反的，b) 对称的，c) 可传递的，d) 反对称的。

(2) 给定 $A=\{1, 2, 3, 4\}$，考虑 A 上的关系 R，若

$$R=\{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle, \langle 3, 4\rangle\}$$

a) 在 $A\times A$ 的坐标图中标出 R，并绘出它的关系图；

b) R 是 i) 自反的，ii) 对称的，iii) 可传递的，iv) 反对称的吗？

(3) 举出 $A=\{1, 2, 3\}$ 上关系 R 的例子，使它有下述性质。

a) 既是对称的又是反对称的；

b) R 既不是对称的，又不是反对称的；

c) R 是可传递的。

(4) 如果关系 R 和 S 是自反的，对称的和可传递的，证明 $R\cap S$ 亦是自反、对称和可传递的。

(5) 给定 $S=\{1, 2, 3, 4\}$ 和 S 上关系 $R=\{\langle 1, 2\rangle, \langle 4, 3\rangle, \langle 2, 2\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle\}$，说明 R 不是可传递的。找出关系 $R_1\supseteq R$，使得 R_1 是可传递的，还能找出另外一个 $R_2\supseteq R$，也是可传递的吗？

(6) 设 R 是集合 X 上的一个自反关系。求证: R 是对称和传递的，当且仅当 $\langle a, b\rangle$ 和 $\langle a, c\rangle$ 在 R 之中则有 $\langle b, c\rangle$ 在 R 之中。

3-7 复合关系和逆关系

二元关系是以序偶为元素的集合，因此对它可以进行集合的运算，如并、交、补等而产生新的集合。对于关系还可以进行一种新的运算，那就是关系的复合。

定义 3-7.1 设 R 为 X 到 Y 的关系，S 为从 Y 到 Z 的关系，则 $R\circ S$ 称为 R 和 S 的复合关系，表示为

$$R\circ S=\{\langle x, z\rangle \mid x\in X\wedge z\in Z\wedge(\exists y)(y\in Y\wedge \langle x, y\rangle\in R\wedge\langle y, z\rangle\in S)\}$$

从 R 和 S，求 $R\circ S$ 称为关系的合成运算。

例如，如果 R_1 是关系“是… 的兄弟”，R_2 是关系“是…的父亲”，那么 $R_1\circ R_2$ 是关系“是…的叔伯”。

又如，如果 R_1 是关系“是…的父亲“，那么 $R_1\circ R_1$ 是关系“是…的祖父”。

合成运算是对关系的二元运算，它能够由两个关系生成一个新的关系，并可以以此类推。

例如 R 是从 X 到 Y 的关系，S 是从 Y 到 Z 的关系，P 是从 Z 到 W 的关系，于是 $(R\circ S)\circ P$ 和 $R\circ(S\circ P)$ 都是从 X 到 W 的关系。容易证明 $(R\circ S)\circ P=R\circ(S\circ P)$，因此关系的合成运算是可结合的。

例题 1 令 $R=\{\langle 1, 2\rangle, \langle 3, 4\rangle, \langle 2, 2\rangle\}$ 和 $S=\{\langle 4, 2\rangle, \langle 2, 5\rangle, \langle 3, 1\rangle, \langle 1, 3\rangle\}$，试求 $R\circ S$, $S\circ R$, $R\circ(S\circ R)$, $(R\circ S)\circ R$, $R\circ R$, $S\circ S$, $R\circ R\circ R$

解 $R\circ S=\{\langle 1, 5\rangle, \langle 3, 2\rangle, \langle 2, 5\rangle\}$

$S\circ R=\{\langle 4, 2\rangle, \langle 3, 2\rangle, \langle 1, 4\rangle\}\neq R\circ S$

$(R\circ S)\circ R=\{\langle 3, 2\rangle\}$

$R\circ(S\circ R)=\{\langle 3, 2\rangle\}$

$R\circ R=\{\langle 1, 2\rangle, \langle 2, 2\rangle\}$

$S\circ S=\{\langle 4, 5\rangle, \langle 3, 3\rangle, \langle 1, 1\rangle\}$

$R \circ R \circ R = \{\langle 1, 2\rangle, \langle 2, 2\rangle\}$

例题 2 设 R_1 和 R_2 是集合 $X = \{0, 1, 2, 3\}$ 上的关系，

$$R_1 = \{\langle i, j\rangle \mid j = i+1 \quad 或 \quad j = \frac{1}{2} i\},$$

$$R_2 = \{\langle i, j\rangle \mid i = j+2\},$$

求 $R_1 \circ R_2$, $R_2 \circ R_1$, $R_1 \circ R_2 \circ R_1$, $R_1 \circ R_1$, $R_1 \circ R_1 \circ R_1$

解：$R_1 = \{\langle 0, 1\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle, \langle 0, 0\rangle, \langle 2, 1\rangle\}$

$R_2 = \{\langle 2, 0\rangle, \langle 3, 1\rangle\}$

$R_1 \circ R_2 = \{\langle 1, 0\rangle, \langle 2, 1\rangle\}$

$R_2 \circ R_1 = \{\langle 2, 1\rangle, \langle 2, 0\rangle, \langle 3, 2\rangle\}$

$R_1 \circ R_2 \circ R_1 = \{\langle 1, 1\rangle, \langle 1, 0\rangle, \langle 2, 2\rangle\}$

$R_1 \circ R_1 = \{\langle 0, 2\rangle, \langle 1, 3\rangle, \langle 1, 1\rangle, \langle 0, 1\rangle, \langle 0, 0\rangle, \langle 2, 2\rangle\}$

$R_1 \circ R_1 \circ R_1 = \{\langle 0, 3\rangle, \langle 0, 1\rangle, \langle 1, 2\rangle, \langle 0, 2\rangle, \langle 0, 0\rangle, \langle 2, 3\rangle, \langle 2, 1\rangle\}$

由关系合成的结合律可以知道关系 R 本身所组成的复合关系可以写成：$R \circ R$, $R \circ R \circ R$, $\cdots$, $\overbrace{R \circ R \circ \cdots \circ R}^{m}$, 分别记作 $R^{(2)}$, $R^{(3)}$, $\cdots$, $R^{(m)}$, 一般地，$\overbrace{R \circ R \circ \cdots \circ R}^{m-1} \circ R = R^{(m-1)} \circ R = R^{(m)}$。

因为关系可用矩阵表示，故复合关系亦可用矩阵表示。已知从集合 $X = \{x_1, x_2, \cdots, x_m\}$ 到集合 $Y = \{y_1, y_2, \cdots, y_n\}$ 有关系 R，则 $M_R = [u_{ij}]$ 表示 R 的关系矩阵，其中，

$$u_{ij} = \begin{cases} 1 & 当 \langle x_i, y_j\rangle \in R \\ 0 & 当 \langle x_i, y_j\rangle \notin R \end{cases}$$

$$(i = 1, 2, \cdots, m; \ j = 1, 2, \cdots, n)$$

同理从集合 $Y = \{y_1, y_2, \cdots, y_n\}$ 到集合 $Z = \{z_1, z_2, \cdots, z_p\}$ 的关系 S，可用矩阵 $M_S = [v_{jk}]$ 表示，其中，

$$v_{jk} = \begin{cases} 1 & 当 \langle y_j, z_k\rangle \in S \\ 0 & 当 \langle y_j, z_k\rangle \notin S \end{cases}$$

$$(j = 1, 2, \cdots, n; \ k = 1, 2, \cdots, p)$$

表示复合关系 $R \circ S$ 的矩阵 $M_{R \circ S}$ 可构造如下：

如果 Y 至少有一个这样的元素 y_j，使得 $\langle x_i, y_j\rangle \in R$ 且 $\langle y_j,$

$z_k\rangle \in S$，则 $\langle x_i, z_k\rangle \in R\circ S$。在集合 Y 中能够满足这样条件的元素可能不止 y_j 一个，例如另有 y'_j 也满足 $\langle x_i, y'_j\rangle \in R$ 且 $\langle y'_j, z_k\rangle \in S$。在所有这样情况下，$\langle x_i, z_k\rangle \in R\circ S$ 都是成立的。这样，当我们扫描 M_R 的第 i 行和 M_S 的第 k 列时，如若发现至少有一个这样的 j，使得此行第 j 个位置上的记入值和第 k 列的第 j 个位置上的记入值都是1时，则在 $M_{R\circ S}$ 的第 i 行和第 k 列 (i, k) 上的记入值亦是1；否则为0。扫描过 M_R 的一行和 M_S 的每一列，就能给出 $M_{R\circ S}$ 的一行，再继续类似的方法就能得到 $M_{R\circ S}$ 的其它各行，因此 $M_{R\circ S}$ 就可用类似于矩阵乘法的方法得到，即

$$M_{R\circ S} = M_R \circ M_S = [w_{ik}],$$

其中

$$w_{ik} = \bigvee_{j=1}^{n} (u_{ij} \wedge v_{jk})。$$

式中 $\vee$ 代表逻辑加，满足 $0\vee 0=0$，$0\vee 1=1$，$1\vee 0=1$，$1\vee 1=1$，

$\wedge$ 代表逻辑乘，满足 $0\wedge 0=0$，$0\wedge 1=0$，$1\wedge 0=0$，$1\wedge 1=1$。

例题3 给定集合 $A=\{1, 2, 3, 4, 5\}$，在集合 A 上定义两种关系。$R=\{\langle 1, 2\rangle, \langle 3, 4\rangle, \langle 2, 2\rangle\}$，$S=\{\langle 4, 2\rangle, \langle 2, 5\rangle, \langle 3, 1\rangle, \langle 1, 3\rangle\}$，求 $R\circ S$ 和 $S\circ R$ 的矩阵。

解

$$M_{R\circ S}=\begin{bmatrix}0&1&0&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&0&1&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\end{bmatrix}$$

$$=\begin{bmatrix}0&0&0&0&1\\0&0&0&0&1\\0&1&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}$$

$$M_{S\circ R}=\begin{bmatrix}0&0&1&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&0\\0&1&0&0&0\\0&1&0&0&0\\0&0&0&0&0\end{bmatrix}$$

关系是序偶的集合，由于序偶的有序性，关系还有一些特殊的运算。

定义 3-7.2 设 R 为 X 到 Y 的二元关系，如将 R 中每一序偶的元素顺序互换，所得到的集合称为 R 的逆关系。记作 R^c，即 $R^c=\{\langle y, x\rangle \mid \langle x, y\rangle \in R\}$。

如在集合 I 上，关系"$<$"的逆关系是"$>$"。而在集合 $X=\{1, 2, 3, 4\}$ 到 $Y=\{a, b, c\}$ 上的关系 $R=\{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, c\rangle\}$，其逆关系为

$$R^c=\{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 3\rangle\}$$

从逆关系的定义，我们容易看出 $(R^c)^c=R$，这是因为 $\langle x, y\rangle \in R \Leftrightarrow \langle y, x\rangle \in R^c \Leftrightarrow \langle x, y\rangle \in (R^c)^c$。

定理 3-7.1 设 R, R_1 和 R_2 都是从 A 到 R 的二元关系，则下列各式成立。

a) $(R_1 \cup R_2)^c=R_1^c \cup R_2^c$

b) $(R_1 \cap R_2)^c=R_1^c \cap R_2^c$

c) $(A \times B)^c=B \times A$

d) $(\overline{R})^c=\overline{R^c}$　　这里 $\overline{R}=A \times B-R$

e) $(R_1-R_2)^c=R_1^c-R_2^c$

证明　a) $\langle x, y\rangle \in (R_1 \cup R_2)^c \Leftrightarrow \langle y, x\rangle \in R_1 \cup R_2$

$$\Leftrightarrow \langle y, x\rangle \in R_1 \vee \langle y, x\rangle \in R_2$$

$$\Leftrightarrow \langle x, y\rangle \in R_1^c \vee \langle x, y\rangle \in R_2^c$$

$$\Leftrightarrow \langle x, y\rangle \in R_1^c \cup R_2^c$$

d) $\langle x, y\rangle \in (\overline{R})^c \Leftrightarrow \langle y, x\rangle \in \overline{R} \Leftrightarrow \langle y, x\rangle \notin B \Leftrightarrow \langle x, y\rangle \notin R^c$

$$\Leftrightarrow \langle x, y\rangle \in \overline{R^c}$$

e) 因为 $R_1-R_2=R_1 \cap \overline{R}_2$，故有

$$(R_1-R_2)^c=(R_1 \cap \overline{R}_2)^c=R_1^c \cap (\overline{R}_2)^c$$

$$=R_1^c \cap \overline{R}_2^c=R_1^c-R_2^c$$

□

定理 3-7.2 设 T 为从 X 到 Y 的关系，S 为从 Y 到 Z 的关系，证明 $(T \circ S)^c=S^c \circ T^c$。

证明 $\langle z, x\rangle \in (T\circ S)^c \Leftrightarrow \langle x, z\rangle \in T\circ S$

$\Leftrightarrow (\exists y)(y\in Y \wedge \langle x, y\rangle \in T \wedge \langle y, z\rangle \in S)$

$\Leftrightarrow (\exists y)(y\in Y \wedge \langle y, x\rangle \in T^c \wedge \langle z, y\rangle \in S^c)$

$\Leftrightarrow \langle z, x\rangle \in S^c\circ T^c$ □

定理 3-7.3 设 R 为 X 上的二元关系,则

a) R 是对称的,当且仅当 $R=R^c$

b) R 是反对称的,当且仅当 $R\cap R^c\subseteq I_X$

证明 a) 因为 R 是对称的,故 $\langle x, y\rangle \in R \Leftrightarrow \langle y, x\rangle \in R \Leftrightarrow \langle x, y\rangle \in R^c$ 所以 $R=R^c$。

反之,若 $R^c=R$。因为 $\langle x, y\rangle \in R \Leftrightarrow \langle y, x\rangle \in R^c \Leftrightarrow \langle y, x\rangle \in R$,所以 R 是对称的。

b) 其证明留作练习。 □

关系 R^c 的图形,是关系 R 图形中将其弧的箭头方向反置。关系 R^c 的矩阵 M_{R^c} 是 M_R 的转置矩阵。

例题 4 给定集合 $X=\{a, b, c\}$,R 是 X 上的二元关系,R 的关系矩阵

$$M_R=\begin{bmatrix}1&0&1\\1&1&0\\1&1&1\end{bmatrix},$$

求 R^c 和 $R\circ R^c$ 的关系矩阵。

解

$$M_{R^c}=\begin{bmatrix}1&1&1\\0&1&1\\1&0&1\end{bmatrix}$$

$$M_{R\circ R^c}=\begin{bmatrix}1&0&1\\1&1&0\\1&1&1\end{bmatrix}\circ\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$$

3-7 习题

(1) 设 R_1 和 R_2 是 A 上的任意关系,说明以下命题的真假,并予以证明。

a) 若 R_1 和 R_2 是自反的,则 $R_1\circ R_2$ 也是自反的;

b) 若 R_1 和 R_2 是反自反的,则 $R_1\circ R_2$ 也是反自反的;

c) 若 R_1 和 R_1 是对称的,则 $R_1\circ R_2$ 也是对称的;

d) 若 R_1 和 R_2 是传递的，则 $R_1 \circ R_2$ 也是传递的。

(2) 证明若 S 为集合 X 上的二元关系。

a) S 是传递的，当且仅当 $(S \circ S) \subseteq S$

b) S 是自反的，当且仅当 $I_X \subseteq S$

c) 证明定理 3-7.3(b)

(3) 设 S 为 X 上的关系，证明若 S 是自反的和传递的，则 $S \circ S = S$，其逆为真吗？

(4) 令 S 为从 X 到 Y 的关系，T 为从 Y 到 Z 的关系。对于 $A \subseteq X$，定义 $S(A) = \{y \mid \langle x, y \rangle \in S \land x \in A\}$。

证明：

a) $S(A) \subseteq Y$

b) $(S \circ T)(A) = T(S(A))$

c) $S(A \cup B) = S(A) \cup S(B)$

d) $S(A \cap B) \subseteq S(A) \cap S(B)$

(5) R 是 A 上的一个二元关系，如果 R 是自反的，则 R^c 一定是自反的吗？如果 R 是对称的，则 R^c 一定是对称的吗？如果 R 是传递的，则 R^c 一定是传递的吗？

(6) 设 R 为集合 X 上的二元关系，R 在 X 上反传递 $\Leftrightarrow (\forall x)(\forall y)(\forall z)$ $(x \in X \land y \in X \land z \in X \land xRy \land yRz \to x\not{R}z)$，

证明 R 是反传递的，当且仅当 $(R \circ R) \cap R = \emptyset$。

(7) 如果 R 是反对称的关系，则在 $R \cap R^c$ 的关系矩阵中有多少非零值。

(8) 设 R, S, T 为集合 X 上关系，证明 $R \circ (S \cup T) = R \circ S \cup R \circ T$。

3-8 关系的闭包运算

上面所讲的关系的合成和关系的逆都可以构成新的关系。我们还可对给定的关系用扩充一些序偶的办法得到具有某些特殊性质的新关系，这就是闭包运算。

定义 3-8.1 设 R 是 X 上的二元关系，如果有另一个关系 R' 满足：

a) R' 是自反的（对称的，可传递的）；

b) $R' \supseteq R$；

c) 对于任何自反的（对称的，可传递的）关系 R''，如果有 R''

$\supseteq R$，就有 $R''\supseteq R'$。则称关系 R' 为 R 的自反(对称，传递)闭包。记作

$$r(R),\ (s(R),\ t(R))$$

对于 X 上的二元关系 R，我们能够用扩充序偶的方法来形成它的自反(对称，传递)闭包，但必须注意，自反(对称，传递)闭包应是包含 R 的最小自反(对称，传递)关系。

定理3-8.1 设 R 是 X 上的二元关系，那么

a) R 是自反的，当且仅当 $r(R)=R$

b) R 是对称的，当且仅当 $s(R)=R$

c) R 是传递的，当且仅当 $t(R)=R$

证明 a) 如果 R 是自反的，因为 $R\supseteq R$，且任何包含 R 的自反关系 R''，有 $R''\supseteq R$，故 R 就满足自反闭包的定义，即

$$r(R)=R$$

反之，如果 $r(R)=R$，根据定义 3-8.1a)，R 必是自反的。

b) 和 c) 的证明完全类似。 □

下面几个定理介绍了由给定关系 R，求 $r(R)$，$s(R)$ 和 $t(R)$ 的方法。

定理3-8.2 设 R 是集合 X 上的二元关系，则

$$r(R)=R\cup I_X$$

证明 令 $R'=R\cup I_X$，对任意 $x\in X$，因为有 $\langle x, x\rangle\in I_X$，故 $\langle x, x\rangle\in R'$，于是 R' 在 X 上是自反的。

又 $R\subseteq R\cup I_X$ 即 $R\subseteq R'$。若有自反关系 R'' 且 $R''\supseteq R$，显然有 $R''\supseteq I_X$，于是

$$R''\supseteq I_X\cup R=R'$$

故

$$r(R)=R\cup I_X$$ □

定理3-8.3 设 R 是集合 X 上的二元关系，则

$$s(R)=R\cup R^c$$

证明 令 $R'=R\cup R^c$，因为 $R\subseteq R\cup R^c$ 即 $R'\supseteq R$，又设 $\langle x, y\rangle\in R'$，则 $\langle x, y\rangle\in R$ 或 $\langle x, y\rangle\in R^c$，即 $\langle y, x\rangle\in R^c$ 或 $\langle y, x\rangle\in R$，故 $\langle y, x\rangle\in R\cup R^c$，所以 R' 是对称的。

设 R'' 是对称的且 $R''\supseteq R$，对任意 $\langle x, y\rangle\in R'$，则 $\langle x, y\rangle\in R$ 或 $\langle x, y\rangle\in R^c$。当 $\langle x, y\rangle\in R$ 则 $\langle x, y\rangle\in R''$，当 $\langle x, y\rangle\in R^c$ 时，$\langle y, x\rangle\in R$，$\langle y, x\rangle\in R''$，因为 R'' 对称，所以 $\langle x, y\rangle\in R''$，因此 $R'\subseteq R''$，故

$$s(R)=R\cup R^c$$ □

定理 3-8.4 设 R 是 X 上的二元关系，则

$$t(R)=\bigcup_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots$$

证明 a) 先证 $\bigcup_{i=1}^{\infty}R^i\subseteq t(R)$，用归纳法。

(1) 根据传递闭包定义 $R\subseteq t(R)$；

(2) 假定 $n\geq 1$ 时，$R^n\subseteq t(R)$，设 $\langle x, y\rangle\in R^{n+1}$。因为 $R^{n+1}=R^n\circ R$，故必有某个 $c\in X$，使 $\langle x, c\rangle\in R^n$ 和 $\langle c, y\rangle\in R$，故有 $\langle x, c\rangle\in t(R)$ 和 $\langle c, y\rangle\in t(R)$ 即 $\langle x, y\rangle\in t(R)$，所以

$$R^{n+1}\subseteq t(R)$$

故
$$\bigcup_{i=1}^{\infty}R^i\subseteq t(R)$$

b) 再证 $t(R)\subseteq\bigcup_{i=1}^{\infty}R^i$。

设 $\langle x, y\rangle\in\bigcup_{i=1}^{\infty}R^i$，$\langle y, z\rangle\in\bigcup_{i=1}^{\infty}R^i$，则必存在整数 s 和 t，使得 $\langle x, y\rangle\in R^s$，$\langle y, z\rangle\in R^t$，这样 $\langle x, z\rangle\in R^s\circ R^t$，即 $\langle x, z\rangle\in\bigcup_{i=1}^{\infty}R^i$，所以 $\bigcup_{i=1}^{\infty}R^i$ 是传递的。

由于包含 R 的可传递关系都包含 $t(R)$，故

$$t(R)\subseteq\bigcup_{i=1}^{\infty}R^i$$

由 a) 和 b) 可得 $t(R)=\bigcup_{i=1}^{\infty}R^i$，通常，将 $\bigcup_{i=1}^{\infty}R^i$ 记作 R^+。 □

例题 1 设 $A=\{a, b, c\}$，R 是 A 上的二元关系，且给定 $R=\{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle\}$，求 $r(R)$，$s(R)$，$t(R)$。

解 $r(R)=R\cup I_A$

$=\{\langle a, b\rangle, \langle b, c\rangle, \langle c, a\rangle, \langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$

$$s(R)=R\cup R^c=\{\langle a,b\rangle,\langle b,a\rangle,\langle b,c\rangle,\langle c,b\rangle,\langle c,a\rangle,\langle a,c\rangle\}$$

为了求得 $t(R)$，先写出

$$M_R=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$$

$$M_{R^2}=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

即 $R^2=\{\langle a,c\rangle,\langle b,a\rangle,\langle c,b\rangle\}$

$$M_{R^3}=M_{R^2}\circ M_R=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\circ\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$R^3=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle\}$

$$M_{R^4}=M_{R^3}\circ M_R=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\circ\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$$

$$R^4=\{\langle a,b\rangle,\langle b,c\rangle,\langle c,a\rangle\}=R$$

继续这个运算有：$R=R^4=\cdots=R^{3n+1}$

$R^2=R^5=\cdots=R^{3n+2}$

$R^3=R^6=\cdots=R^{3n+3}\ (n=1,2,\cdots)$

故
$$t(R)=\bigcup_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots=R\cup R^2\cup R^3$$
$$=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle,\langle a,b\rangle,\langle b,c\rangle,\langle c,a\rangle,\langle a,c\rangle,\langle b,a\rangle,\langle c,b\rangle\}$$

$$M_{t(R)}=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$$

从例题1中看到给定 X 上关系 R 求 $t(R)$，有时不必求出每一R^i，下面定理指出了计算 $t(R)$ 与集合 X 中元素个数的联系。

定理3-8.5 设 X 是含有 n 个元素的集合，R 是 X 上的二元关系，则存在一个正整数 $k\leqslant n$，使得

$$t(R)=R\cup R^2\cup R^3\cup\cdots\cup R^k$$

证明　设有 x_i，$x_j\in X$，记 $t(R)=R^+$，如果 $x_iR^+x_j$ 成立则

存在整数 $p>0$，使得 $x_iR^px_j$ 成立，即存在序列 $e_1, e_2, \cdots, e_{p-1}$ 有 $x_iRe_1, e_1Re_2, \cdots, e_{p-1}Rx_j$。设满足上述条件的最小 p 大于 n，则在上述序列中必有 $0\leqslant t<q\leqslant p$，使 $e_t=e_q$，因此序列就成为

$$\underbrace{x_iRe_1,\ e_1Re_2,\ \cdots,\ e_{t-1}Re_t}_{t\text{个}},\ \underbrace{e_tRe_{q+1},\ \cdots,\ e_{p-1}Rx_j}_{(p-q)\text{个}}$$

这表明 $x_iR^kx_j$ 存在，其中 $k=t+p-q=p-(q-t)<p$，这与 p 是最小的假设矛盾，故 $p>n$ 不成立。 □

从本定理可以知道，在 n 个元素的有限集上关系 R 的传递闭包不妨写为 $t(R)=R\cup R^2\cup\cdots\cup R^n$。

例题 2 设 $A=\{a, b, c, d\}$，给定 A 上的关系 R 为 $R=\{\langle a,b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$，求 $t(R)$。

解

$$M_R=\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{bmatrix}$$

$$M_{R^2}=\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{bmatrix}=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

$$M_{R^3}=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&0&0\\0&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{bmatrix}=\begin{bmatrix}0&1&0&1\\1&0&1&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

$$M_{R^4}=\begin{bmatrix}0&1&0&1\\1&0&1&0\\0&0&0&0\\0&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{bmatrix}=\begin{bmatrix}1&0&1&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

所以

$$M_{t(R)}=\begin{bmatrix}1&1&1&1\\1&1&1&1\\0&0&0&1\\0&0&0&0\end{bmatrix}$$

当有限集 X 的元素较多时，对关系 R 的传递闭包 R^+ 进行矩

阵运算,显得很为繁琐,为此 Warshall 在 1962 年提出了 R^+ 的一个有效算法如下:

(1) 置新矩阵 $A:=M$;

(2) 置 $i:=1$;

(3) 对所有 j 如果 $A[j, i]=1$, 则对 $k=1, 2, \cdots, n$

$$A[j, k]:=A[j, k]+A[i, k];$$

(4) i 加 1;

(5) 如果 $i\leqslant n$, 则转到步骤(3),否则停止。

例题 3

已知 $M=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ 求 $t(R)$。

解

$$A:=M=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$i=1$ 时, 第一列中只有 $A[1, 1]=1$, 将第一行与第一行各对应元素进行逻辑加,仍记于第一行得:

$$A:=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$i=2$ 时,第二列中 $A[1, 2]=1$, $A[4, 2]=1$, 分别将第一行、第四行各元

素和第二行各对应元素逻辑相加，仍分别记于第一行和第四行得：

$$A:=\begin{bmatrix}1&1&0&1&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&1&0&0\\0&1&0&1&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\end{bmatrix}$$

$i=3$ 时，第三列中没有不等于零的元素，A 的赋值不动。

$i=4$ 时，第四列中 $A[1,4]=A[2,4]=A[4,4]=1$，将一、二、四这三行和第四行对应元素逻辑相加，仍分别记于一、二、四这三行得：

$$A:=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&0&1&0&0&0\\0&0&0&0&1&0&0\\0&1&0&1&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\end{bmatrix}$$

$i=5$ 时，$A[3,5]=1$，将第三行与第五行的对应元素逻辑相加，仍记于第三行，由于第五行的元素都等于零，A 的赋值不变。

$i=6$，$i=7$ 时，由于第六、七列各元素均为零，A 的赋值不变。

$$M_{R^+}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&0&1&0&0&0\\0&0&0&0&1&0&0\\0&1&0&1&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\end{bmatrix}$$

传递闭包 R^+ 在语法分析中有很多应用，现以下例说明。

例题 4 设有一字母表 $V=\{A,B,C,D,e,d,f\}$ 并给定下面六条规则。

$$A\to Af,\ B\to Dde,\ C\to e$$

$$A\to B,\ B\to De,\ D\to Bf$$

R 为定义在 V 上的二元关系且 x_iRx_j，即是从 x_i 出发用一条规则推出一串字符，使其第一个字符恰为 x_j。说明每个字母连续应用上述规则可能推出的头字符。

解　R 的关系矩阵为:

$$M_R=\begin{array}{c} \\ A \\ B \\ C \\ D \\ e \\ d \\ f \end{array}\begin{array}{c} \begin{matrix} A & B & C & D & e & d & f \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

则 $x_iR^+x_j$ 表示从 x_i 出发，经过多次连续推导而得的字符串，其第一个字符恰为 x_j 的关系，此关系即是上例中计算的 M_{R^+}。

$$M_{R^+}=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

因此 $R^+=\{\langle A, A\rangle, \langle A, B\rangle, \langle A, D\rangle, \langle B, B\rangle, \langle B, D\rangle, \langle C, e\rangle, \langle D, B\rangle, \langle D, D\rangle\}$。

这说明应用给定的六条规则，从 A 出发推导的头字符有 A、B、D 三种可能，而从 B 出发推导的头字符有 B、D 两种可能，而从 D 推出的头字符有 B、D 两种可能，从 C 出发推导的头字符只可能为 e。

关系 R 的自反(对称，传递)闭包还可以进一步复合成自反(对称、传递)等闭包，它们之间有如下定理：

定理3-8.6　设 X 是集合，R 是 X 上的二元关系，则

a) $rs(R)=sr(R)$

b) $rt(R)=tr(R)$

c) $ts(R)\supseteq st(R)$

证明　令 I_X 表示 X 上的恒等关系。

a)
$$\begin{aligned} sr(R) &= s(I_X\cup R)=(I_X\cup R)\cup(I_X\cup R)^c \\ &= (I_X\cup R)\cup(I_X^c\cup R^c)=I_X\cup R\cup R^c \\ &= I_X\cup s(R)=rs(R) \end{aligned}$$

b) $$tr(R)=t(I_X\cup R)=\bigcup_{i=1}^{\infty}(I_X\cup R)^i=\bigcup_{i=1}^{\infty}\left(I_X\cup\bigcup_{j=1}^{i}R^j\right)$$
$$=I_X\cup\bigcup_{i=1}^{\infty}\bigcup_{j=1}^{i}R^j=I_X\cup\bigcup_{i=1}^{\infty}R^i$$
$$=I_X\cup t(R)=rt(R)$$

c) 其证明并不困难，留作练习请读者自证。 □

3-8 习题

(1) 根据图 3-8.1 中的有向图，写出邻接矩阵和关系 R，并求出 R 的自反闭包和对称闭包。

(2) 设集合 $A=\{a, b, c, d\}$，A 上的关系

$$R=\{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$$

a) 用矩阵运算和作图方法求出 R 的自反闭包，对称闭包和传递闭包；

b) 用 Warshall 算法求出 R 的传递闭包。

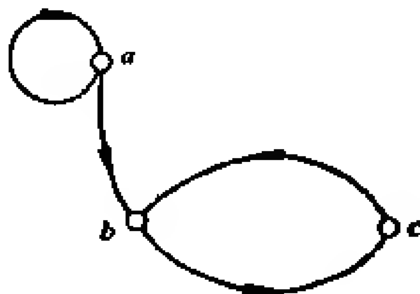


图 3-8.1

(3) 归纳出用矩阵和作图方法求出自反(对称，传递)闭包的一般方法。

(4) 设 R 是有限集 X 上的一个二元关系，证明：

a) 对于任意在 X 上的二元关系 R，有 R^+ 是可传递的；

b) 若有 X 上任何其它传递关系 P，使得 $P\supseteq R$，则必有 $R^+\subseteq P$；

c) R^+ 就是定义 3-8.1 中所说的传递闭包。

(5) 设 R_1 和 R_2 是集合 A 上的关系且 $R_1\supseteq R_2$，求证

a) $r(R_1)\supseteq r(R_2)$

b) $s(R_1)\supseteq s(R_2)$

c) $t(R_1)\supseteq t(R_2)$

(6) 证明定理 3-9.6 的 c)。

(7) 设 R_1 和 R_2 是 A 上的关系，证明

a) $r(R_1\cup R_2)=r(R_1)\cup r(R_2)$

b) $s(R_1\cup R_2)=s(R_1)\cup s(R_2)$

c) $t(R_1\cup R_2)\supseteq t(R_1)\cup t(R_2)$

(8) 设 R 是集合 A 上的一个任意关系，$R^*=tr(R)$，证明下列各式：

a) $(R^+)^+ = R^+$

b) $R \cdot R^* = R^+ = R^* \cdot R$

c) $(R^*)^* = R^*$

3-9 集合的划分和覆盖

在集合的研究中，除了常常把两个集合相互比较之外，有时也要把一个集合分成若干子集加以讨论。

定义 3-9.1 若把一个集合 A 分成若干个叫做分块的非空子集，使得 A 中每个元素至少属于一个分块，那么这些分块的全体构成的集合叫做 A 的一个覆盖。如果 A 中每个元素属于且仅属于一个分块，那么这些分块的全体构成的集合叫做 A 的一个划分(成分划)。

上述定义与下面的定义是等价的。

定义 3-9.1′ 令 A 为给定非空集合，$S=\{S_1, S_2, \cdots, S_m\}$ 其中 $S_i \subseteq A$，$S_i \neq \emptyset (i=1, 2, \cdots, m)$ 且 $\bigcup_{i=1}^{m} S_i = A$，集合 S 称作集合 A 的覆盖。

如果除以上条件外，另有 $S_i \cap S_j = \emptyset (i \neq j)$ 则称 S 是 A 的划分(或分划)。

例如，$A=\{a, b, c\}$，考虑下列子集：

$S=\{\{a, b\}, \{b, c\}\}$，$Q=\{\{a\}, \{a, b\}, \{a, c\}\}$

$D=\{\{a\}, \{b, c\}\}$，　$G=\{\{a, b, c\}\}$

$E=\{\{a\}, \{b\}, \{c\}\}$，$F=\{\{a\}, \{a, c\}\}$

则 S、Q 是 A 的覆盖，D、G、E 是 A 的划分，F 既不是划分也不是覆盖。显然，若是划分则必是覆盖，其逆不真。任一个集合的最小划分，就是由这个集合的全部元素组成的一个分块的集合。如上例中，G 是 A 的最小划分。

任一个集合的最大划分是由每个元素构成一个单元素分块的集合，如上例中，E 是 A 的最大划分。

需要注意：

给定集合 A 的划分并不是唯一的。但是已知一个集合却很容易构造出一种划分。

定义 3-9.2 若 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 是同一集合 A 的两种划分，则其中所有 $A_i \cap B_j$ 组成的集合，称为是原来两种划分的交叉划分。

例如，所有生物的集合 X，可分割成 $\{P, A\}$，其中 P 表示所有植物的集合，A 表示所有动物的集合，又 X 也可构成 $\{E, F\}$，其中 E 表示史前生物，F 表示史后生物，则其交叉划分为 $Q=\{P\cap E, P\cap F, A\cap E, A\cap F\}$，其中 $P\cap E$ 表示史前植物，$P\cap F$ 表示史后植物，$A\cap E$ 表示史前动物，$A\cap F$ 表示史后动物。

定理 3-9.1 设 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 是同一集合 X 的两种划分，则其交叉划分亦是原集合的一种划分。

证明 因为题设的交叉划分是：

$$\{A_1\cap B_1, A_1\cap B_2, \cdots, A_1\cap B_s,$$
$$A_2\cap B_1, A_2\cap B_2, \cdots, A_2\cap B_s, \cdots,$$
$$A_r\cap B_1, A_r\cap B_2, \cdots, A_r\cap B_s\},$$

在交叉划分中，任取两元素，$A_i\cap B_h$，$A_j\cap B_k$，考察 $(A_i\cap B_h)\cap(A_j\cap B_k)$，

I：若 $i\neq j$ 且 $h=k$，因为 $A_i\cap A_j=\emptyset$ 故

$$A_i\cap B_h\cap A_j\cap B_k=\emptyset\cap B_h\cap B_k=\emptyset$$

II：若 $i\neq j$ 且 $h\neq k$，因为 $A_i\cap A_j=\emptyset$，$B_h\cap B_k=\emptyset$ 故

$$A_i\cap B_h\cap A_j\cap B_k=\emptyset\cap\emptyset=\emptyset$$

III：$i=j$ 且 $h\neq k$，情况与 I 相同。

综上所述，在交叉划分中，任取两元素，其交为

$$A_i\cap B_h\cap A_j\cap B_k=\emptyset$$

其次，交叉划分中所有元素的并为

$$
\begin{aligned}
&(A_1\cap B_1)\cup(A_1\cap B_2)\cup\cdots\cup(A_1\cap B_s)\cup\cdots\\
&\quad\cup(A_r\cap B_1)\cup(A_r\cap B_2)\cup\cdots\cup(A_r\cap B_s)\\
&=(A_1\cap(B_1\cup B_2\cup\cdots\cup B_s))\cup(A_2\cap(B_1\cup B_2\cup\cdots\\
&\quad\cup B_s))\cdots(A_r\cap(B_1\cup B_2\cup\cdots\cup B_s))\\
&=((A_1\cup A_2\cup\cdots\cup A_r)\cap(B_1\cup B_2\cup\cdots\cup B_s))\\
&=X\cap X=X
\end{aligned}
$$
□

定义 3-9.3 给定 X 的任意两个划分 $\{A_1, A_2, \cdots, A_r\}$ 和 $\{B_1, B_2, \cdots, B_s\}$，若对于每一个 A_j 均有 B_k 使 $A_j\subseteq B_k$，则 $\{A_1, A_2, \cdots, A_r\}$ 称为是 $\{B_1, B_2, \cdots, B_s\}$ 的加细。

定理 3-9.2 任何两种划分的交叉划分，都是原来各划分的一种加细。

证明 设 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 的交叉划分为 T，对 T 中任意元素 $A_i\cap B_j$ 必有 $A_i\cap B_j\subseteq A_i$ 和 $A_i\cap B_j\subseteq B_j$，故 T 必是原划分的加细。 □

3-9 习题

(1) 4个元素的集合共有多少个不同的划分?

(2) 设 $\{A_1, A_2, \cdots, A_k\}$ 是集合 A 的一个划分，我们定义 A 上的一个二元关系 R，使 $\langle a, b\rangle\in R$ 当且仅当 a 和 b 在这个划分的同一块中，证明：R 是自反的、对称的和传递的。

(3) 设 π_1 和 π_2 是非空集合 A 的划分，说明下列各式哪些是 A 的划分，哪些可能是 A 的划分，哪些不是 A 的划分，并给予证明。

a) $\pi_1\cup\pi_2$

b) $\pi_1\cap\pi_2$

c) $\pi_1-\pi_2$

(4) 设 R 是集合 A 上的一个自反、对称和传递的关系。若 $\{A_1, A_2, \cdots, A_k\}$ 是 A 的子集的集合，当 $i\neq j$ 时，$A_i\not\subseteq A_j$，使 a 和 b 在一个子集中当且仅当 $\langle a, b\rangle\in R$，求证 $\{A_1, A_2, \cdots, A_k\}$ 是 A 的一个划分。

(5) 设 $\{A_1, A_2, \cdots, A_n\}$ 是集合 A 的划分，若 $A_i\cap B\neq\emptyset$，$1\leq i\leq n$，试证明 $\{A_1\cap B, A_2\cap B, \cdots, A_n\cap B\}$ 是集合 $A\cap B$ 的划分。

3-10　等价关系与等价类

下面介绍具有特别重要意义的一类二元关系，等价关系。

定义 3-10.1　设 R 为定义在集合 A 上的一个关系，若 R 是自反的，对称的和传递的，则 R 称为等价关系。

例如平面上三角形集合中，三角形的相似关系是等价关系；上海市的居民的集合中，住在同一区的关系也是等价关系。

例题 1　设集合 $T=\{1, 2, 3, 4\}$，$R=\{\langle 1, 1\rangle, \langle 1, 4\rangle, \langle 4, 1\rangle, \langle 4, 4\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$。

验证 R 是 T 上的等价关系。

解　画出 R 的关系矩阵与关系图 3-10.1

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

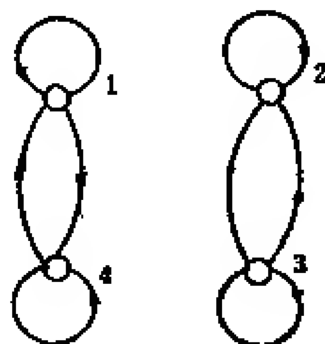


图 3-10.1

每一结点都有自回路，说明R是自反的。任意两结点间或没有弧线连接，或有成对弧出现，故 R 是对称的。从 R 的序偶表示式中，可以看出 R 是传递的，逐个检查序偶，如 $\langle 1, 1\rangle\in R$, $\langle 1, 4\rangle\in R$，有 $\langle 1, 4\rangle\in R$。同理 $\langle 1, 4\rangle\in R$, $\langle 4, 1\rangle\in R$，有 $\langle 1, 1\rangle\in R$, …。故 R 是 T 上的等价关系。

同样地，从关系矩阵亦可验证 R 是等价关系。

例题 2　设 I 为整数集，$R=\{\langle x, y\rangle | x\equiv y(\mathrm{mod}\, k)\}$，证明 R 是等价关系。

证明　设任意 $a, b, c\in I$

Ⅰ．因为 $a-a=k\cdot 0$，所以　$\langle a, a\rangle\in R$

Ⅱ．若 $a\equiv b(\mathrm{mod}\, k)$，$a-b=kt$（$t$ 为整数），则 $b-a=-kt$，所以

$$b\equiv a(\mathrm{mod}\, k)$$

Ⅲ．若 $a\equiv b(\mathrm{mod}\, k)$，$b\equiv c(\mathrm{mod}\, k)$，则 $a-b=kt$, $b-c=ks$（t, s 为整数），$a-c=a-b+b-c=k(t+s)$，所以　$a\equiv c(\mathrm{mod}\, k)$

因此 R 是等价关系。

定义 3-10.2　设 R 为集合 A 上的等价关系，对任何 $a\in A$，集合 $[a]_R=\{x|x\in A, aRx\}$ 称为元素 a 形成的 R 等价类。

由等价类的定义可知$[a]_R$是非空的，因为$a\in[a]_R$，因此任给集合A及其上的等价关系R，必可写出A上各个元素的等价类，例如在例题1中，T的各个元素的等价类为：

$$[1]_R=[4]_R=\{1,4\}$$
$$[2]_R=[3]_R=\{2,3\}$$

例题3 设I是整数集合，R是同余模3的关系，即

$$R=\{\langle x,y\rangle|x\in I,y\in I,x\equiv y(\bmod 3)\}$$

确定由I的元素所产生的等价类。

解 由例题2中已证明整数集合上的同余模k的关系是等价关系，故本例中由I的元素所产生的等价类是

$$[0]_R=\{\cdots,-6,-3,0,3,6,\cdots\}$$
$$[1]_R=\{\cdots,-5,-2,1,4,7,\cdots\}$$
$$[2]_R=\{\cdots,-4,-1,2,5,8,\cdots\}$$

从例题3可以看到，在集合I上同余模3等价关系R所构成的等价类有：

$$[0]_R=[3]_R=[-3]_R=\cdots$$
$$[1]_R=[4]_R=[-2]_R=\cdots$$
$$[2]_R=[5]_R=[-1]_R=\cdots$$

定理3-10.1 设给定集合A上的等价关系R，对于$a,b\in A$有aRb iff $[a]_R=[b]_R$。

证明 假定$[a]_R=[b]_R$，因为$a\in[a]_R$，故$a\in[b]_R$，即aRb。

反之，若aRb，设

$$c\in[a]_R\Rightarrow aRc\Rightarrow cRa\Rightarrow cRb\Rightarrow c\in[b]_R$$

即
$$[a]_R\subseteq[b]_R$$

同理，若$c\in[b]_R\Rightarrow bRc\Rightarrow aRc\Rightarrow c\in[a]_R$，故$[b]_R\subseteq[a]_R$，

由此证得若aRb，则$[a]_R=[b]_R$。 □

定义3-10.3 集合A上的等价关系R，其等价类集合$\{[a]_R|a\in A\}$称作A关于R的商集，记作A/R。

如例题1中商集$T/R=\{[1]_R,[2]_R\}$，例题3中商集

$$I/R=\{[0]_R,[1]_R,[2]_R\}。$$

我们注意到商集 I/R 中，$[0]_R\cup[1]_R\cup[2]_R=I$，且任意两个等价类的交为 $\emptyset$。于是我们有下述重要定理。

定理 3-10.2 集合 A 上的等价关系 R，决定了 A 的一个划分，该划分就是商集 A/R。

证明 设集合 A 上有一个等价关系 R，把与 A 的固定元 a 有等价关系的元素放在一起作成一个子集 $[a]_R$，则所有这样的子集做成商集 A/R。

I：在 $A/R=\{[a]_R|a\in A\}$ 中，$\bigcup\limits_{a\in A}[a]_R=A$。

II：对于 A 的每一个元素 a，由于 R 是自反的，故必有 aRa 成立，即 $a\in[a]_R$，故 A 的每个元素的确属于一个分块。

III：A 的每个元素只能属于一个分块。

反证 若 $a\in[b]_R$，$a\in[c]_R$，且 $[b]_R\neq[c]_R$，则 bRa，cRa 成立，由对称性得 aRc 成立，再由传递性得 bRc，据定理 3-10.1 必有 $[b]_R=[c]_R$，这与题设矛盾。故 A/R 是 A 上对应于 R 的一个划分。 □

定理 3-10.3 集合 A 的一个划分确定 A 的元素间的一个等价关系。

证明 设集合 A 有一个划分 $S=\{S_1, S_2, \cdots, S_m\}$，现定义一个关系 R，aRb 当且仅当 a，b 在同一分块中。可以证明这样规定的关系 R 是一个等价关系。因为

I：a 与 a 在同一分块中，故必有 aRa。即 R 是自反的。

II：若 a 与 b 在同一分块，b 与 a 也必在同一分块中，即 $aRb\Rightarrow bRa$，故 R 是对称的。

III：若 a 与 b 在同一分块中，b 与 c 在同一分块中，因为

$$S_i\cap S_j=\emptyset\ (i\neq j)$$

即 b 属于且仅属于一个分块，故 a 与 c 必在同一分块中，故有

$$(aRb)\wedge(bRc)\Rightarrow(aRc)$$

即 R 是传递的。R 满足上述三个条件，故 R 是等价关系，由 R 的定义可知，S 就是 A/R。 □

例题4 设 $A=\{a, b, c, d, e\}$，有一个划分 $S=\{\{a, b\}, \{c\}, \{d, e\}\}$，试由划分 S 确定 A 上的一个等价关系 R。

解 我们用如下办法产生一个等价关系 R

$$R_1=\{a, b\}\times\{a, b\}=\{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle\}$$

$$R_2=\{c\}\times\{c\}=\{\langle c, c\rangle\}$$

$$R_3=\{d, e\}\times\{d, e\}=\{\langle d, d\rangle, \langle d, e\rangle, \langle e, d\rangle, \langle e, e\rangle\}$$

$$R=R_1\cup R_2\cup R_3=\{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle d, d\rangle, \langle e, e\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle d, e\rangle, \langle e, d\rangle\}$$

从 R 的序偶表示式中，容易验证 R 是等价关系。

应该注意，本例中确定 R 的方法与定理 3-10.3 中所述确定等价关系方法实质相同。

定理 3-10.4 设 R_1 和 R_2 为非空集合 A 上的等价关系，则 $R_1=R_2$ 当且仅当 $A/R_1=A/R_2$。

证明 因为 $A/R_1=\{[a]_{R_1}|a\in A\}$

$$A/R_2=\{[a]_{R_2}|a\in A\}$$

若 $R_1=R_2$，对任意 $a\in A$，则.

$$[a]_{R_1}=\{x|x\in A, aR_1x\}=\{x|x\in A, aR_2x\}=[a]_{R_2}$$

故 $\{[a]_{R_1}|a\in A\}=\{[a]_{R_2}|a\in A\}$，即 $A/R_1=A/R_2$

反之，假设 $\{[a]_{R_1}|a\in A\}=\{[a]_{R_2}|a\in A\}$

对任意 $[a]_{R_1}\in A/R_1$，必存在 $[c]_{R_2}\in A/R_2$，使得 $[a]_{R_1}=[c]_{R_2}$，故

$$\langle a, b\rangle\in R_1\Leftrightarrow a\in[a]_{R_1}\wedge b\in[a]_{R_1}\Leftrightarrow a\in[c]_{R_2}\wedge b\in[c]_{R_2}$$

$$\Rightarrow\langle a, b\rangle\in R_2$$

所以，$R_1\subseteq R_2$，类似地有 $R_2\subseteq R_1$，因此，$R_1=R_2$。 □

3-10 习题

(1) 设 R 和 R' 是集合 A 上的等价关系，用例子证明 $R\cup R'$ 不一定是等价关系。

(2) 试问由 4 个元素组成的有限集上所有的等价关系的个数为多少？

(3) 给定集合 $S=\{1, 2, 3, 4, 5\}$，找出 S 上的等价关系 R，此关系 R 能够产生划分 $\{\{1, 2\}, \{3\}, \{4, 5\}\}$ 并画出关系图。

(4) 设 R 是一个二元关系，设 $S=\{\langle a, b\rangle|$对于某一 c，有 $\langle a, c\rangle\in R$ 且

$\langle c, b\rangle \in R\}$，证明若 R 是一个等价关系，则 S 也是一个等价关系。

(5) 设正整数的序偶集合 A，在 A 上定义的二元关系 R 如下：$\langle\langle x, y\rangle, \langle u, v\rangle\rangle \in R$，当且仅当 $xv=yu$，证明 R 是一个等价关系。

(6) 设 R 是集合 A 上的对称和传递关系，证明如果对于 A 中的每一个元素 a，在 A 中同时也存在一个 b，使 $\langle a, b\rangle$ 在 R 之中，则 R 是一个等价关系。

(7) 设 R_1 和 R_2 是非空集合 A 上的等价关系，确定下述各式，哪些是 A 上的等价关系，对不是的提供反例证明。

a) $(A\times A)-R_1$

b) R_1-R_2

c) R_1^2

d) $r(R_1-R_2)$（即 R_1-R_2 的自反闭包）。

(8) 设 C^* 是实数部分非零的全体复数组成的集合，C^* 上关系 R 定义为：$(a+b_i)R(c+d_i)\Leftrightarrow ac>0$，证明 R 是等价关系，并给出关系 R 的等价类的几何说明。

(9) 设 π 和 π' 是非空集合 A 上的划分，并设 R 和 R' 是分别由 π 和 π' 诱导的等价关系，那么，π' 细分 π 的充要条件是 $R'\subseteq R$。

(10) 设 R_j 表示 I 上的模 j 等价关系，R_k 表示 I 上的模 k 等价关系，证明 I/R_k 细分 I/R_j 当且仅当 k 是 j 的整数倍。

3-11 相 容 关 系

与等价关系一样，另一类应用非常广泛的关系，就是相容关系。

定义 3-11.1 给定集合 A 上的关系 r，若 r 是自反的，对称的，则称 r 是相容关系。

例如，设 A 是由下列英文单词组成的集合。

$A=\{$cat, teacher, cold, desk, knife, by$\}$

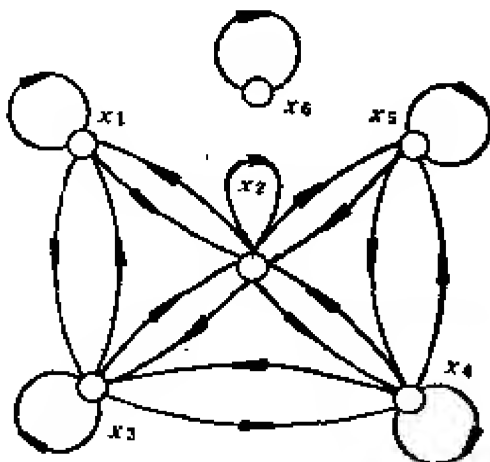


图 3-11.1

定义关系：

$r=\{\langle x, y\rangle | x,y\in A$ 且 x 和 y 有相同的字母$\}$。显然，r 是一个

相容关系。

令 $x_1=\text{cat}$, $x_2=\text{teacher}$, $x_3=\text{cold}$, $x_4=\text{desk}$, $x_5=\text{knife}$, $x_6=\text{by}$。

r 的关系图可由图 3–11.1 表示。

$$
r\text{ 的关系矩阵为 } M_r=\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}
$$

由于相容关系是自反和对称的，因此其关系矩阵的对角线元素都是 1，且矩阵是对称的。为此我们可将矩阵用梯形表示。

同理，在相容关系的关系图上，每个结点处都有自回路且每两个相关结点间的弧线都是成对出现的。为了简化图形，我们今后对相容关系图，不画自回路，并用单线代替来回弧线，因此上例的关系矩阵和关系图可简化为表 3–11.1 和图 3–11.2。

表 3–11.1

x_2	1				
x_3	1	1			
x_4	0	1	1		
x_5	0	1	0	1	
x_6	0	0	0	0	0
	x_1	x_2	x_3	x_4	x_5

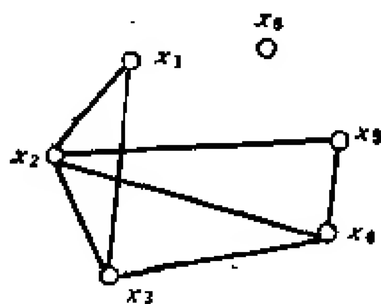


图 3–11.2

定义 3–11.2 设 r 是集合 A 上的相容关系，若 $C\subseteq A$，如果对于 C 中任意两个元素 a_1, a_2 有 a_1ra_2，称 C 是由相容关系 r 产生的相容类。

例如上例的相容关系 r 可产生相容类 $\{x_1, x_2\}$，$\{x_1, x_3\}$，$\{x_2, x_3\}$，$\{x_6\}$，$\{x_2, x_4, x_5\}$ 等等。

对于前三个相容类，都能加进新的元素组成新的相容类；而后

两个相容类，加入任一新元素，就不再组成相容类，我们称它为最大相容类。

定义 3-11.3 设 r 是集合 A 上的相容关系，不能真包含在任何其它相容类中的相容类，称作最大相容类。记作 C_r。

若 C_r 为最大相容类，显然它是 A 的子集，对于任意 $x\in C_r$，x 必与 C_r 中所有元素有相容关系。而在 $A-C_r$ 中没有任何元素与 C_r 所有元素有相容关系。

在相容关系图中，最大完全多边形的顶点集合，就是最大相容类。所谓完全多边形，就是其每个顶点都与其它顶点连接的多边形。例如一个三角形是完全多边形，一个四边形加上两条对角线就是完全多边形。

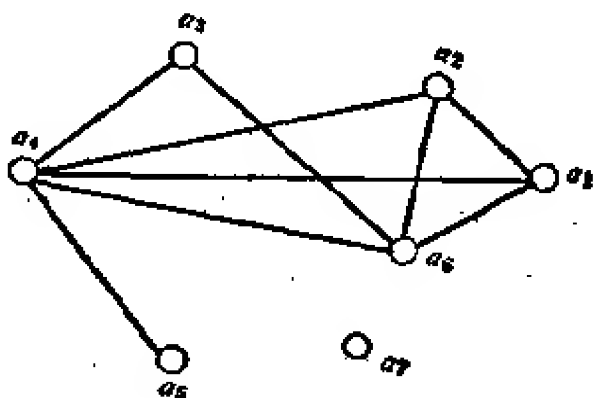


图 3-11.3

此外，在相容关系图中，一个孤立结点，以及不是完全多边形边的两个结点的连线，也是最大相容类。

例题 1 设给定相容关系图如图 3-11.3，写出最大相容类。

解 最大相容类为：

$$\{a_1, a_2, a_4, a_6\}, \{a_3, a_4, a_6\}, \{a_4, a_5\}, \{a_7\}$$

定理 3-11.1 设 r 是有限集 A 上的相容关系，C 是一个相容类，那么必存在一个最大相容类 C_r，使得 $C\subseteq C_r$。

证明 设 $A=\{a_1, a_2, \cdots, a_n\}$，构造相容类序列

$$C_0\subset C_1\subset C_2\subset\cdots, \quad 其中 \quad C_0=C$$

且 $C_{i+1}=C_i\cup\{a_j\}$，其中 j 是满足 $a_j\notin C_i$ 而 a_j 与 C_i 中各元素都有相容关系的最小足标。

由于 A 的元素个数 $|A|=n$，所以至多经过 $n-|C|$ 步，就使这个过程终止，而此序列的最后一个相容类，就是所要找的最大相容类。 □

从定理 3-11.1 中可以看到，A 中任一元素 a，它可以组成相

容类 $\{a\}$，因此必包含在一个最大相容类 C_r 中，因此如由所有最大相容类作出一个集合，则 A 中每一元素至少属于该集合的一个成员之中，所以最大相容类集合必覆盖集合 A。

定义 3-11.4 在集合 A 上给定相容关系 r，其最大相容类的集合称作集合 A 的完全覆盖，记作 $C_r(A)$。

我们注意到集合 A 的覆盖不是唯一的，因此给定相容关系 r，可以作成不同的相容类的集合，它们都是 A 的覆盖。但给定相容关系 r，只能对应唯一的完全覆盖。如例题 1 中，给定 A 上相容关系则有唯一的完全覆盖：$\{\{a_1, a_2, a_4, a_6\}, \{a_3, a_4, a_6\}, \{a_4, a_5\}, \{a_7\}\}$。

定理 3-11.2 给定集合 A 的覆盖 $\{A_1, A_2, \cdots, A_n\}$，由它确定的关系 $R = A_1 \times A_1 \cup A_2 \times A_2 \cup \cdots \cup A_n \times A_n$ 是相容关系。

证明 因为 $A = \bigcup_{i=1}^{n} A_i$，对于任意 $x \in A$，必存在某个 $j > 0$ 使得 $x \in A_j$，所以 $\langle x, x\rangle \in A_j \times A_j$，即 $\langle x, x\rangle \in R$，因此 R 是自反的。

其次，若有任意 $x, y \in A$ 且 $\langle x, y\rangle \in R$，则必存在某个 $h > 0$ 使 $\langle x, y\rangle \in A_h \times A_h$，故必有 $\langle y, x\rangle \in A_h \times A_h$，即 $\langle y, x\rangle \in R$，所以 R 是对称的。

因此证得 R 是 A 上的相容关系。 □

从上述定理可以看到，给定集合 A 上的任意一个覆盖，必可在 A 上构造对应于此覆盖的一个相容关系，但是不同的覆盖却能构造相同的相容关系。

例如，设 $A = \{1, 2, 3, 4\}$，集合 $\{\{1, 2, 3\}, \{3, 4\}\}$ 和 $\{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{3, 4\}\}$ 都是 A 的覆盖，但它们可以产生相同的相容关系。

$$\begin{aligned} r = \{&\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \\ &\langle 2, 3\rangle, \langle 3, 2\rangle, \langle 1, 3\rangle, \langle 3, 1\rangle, \\ &\langle 3, 3\rangle, \langle 4, 4\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle\} \end{aligned}$$

定理 3-11.3 集合 A 上相容关系 r 与完全覆盖 $C_r(A)$ 存在

一一对应。

这个定理的证明留作习题。 □

3-11 习题

(1) 设 R 是 X 上的二元关系，试证明 $\alpha=I_X\cup R\cup R^c$ 是 X 上的相容关系。

(2) 给定集合 $X=\{x_1, x_2, \cdots, x_6\}$，$R$ 是 X 上的相容关系且 M_R 简化矩阵为：

x_2	1				
x_3	1	1			
x_4	0	0	1		
x_5	0	0	1	1	
x_6	1	0	1	0	1
	x_1	x_2	x_3	x_4	x_5

试求出 X 的完全覆盖，并画出相容关系图。

(3) 给定 X 上的相容关系 R，证明 $\bigcup_{i=1}^{\infty} R^i$ 为 X 上的等价关系。

(4) 设 $C=\{A_1, A_2, \cdots, A_n\}$ 为集合 A 的覆盖，试由此覆盖确定 A 上的一个相容关系。并说明在什么条件下，此相容关系为等价关系。

(5) 设 $A=\{1, 2, 3, 4, 5, 6\}$ 上有关系 $\beta=\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle, \langle 3, 4\rangle, \langle 2, 5\rangle, \langle 4, 5\rangle, \langle 3, 6\rangle, \langle 4, 6\rangle\}$。

证明至少有 A 的两个不同覆盖可以产生

$$\alpha=I_X\cup\beta\cup\beta^c$$

(6) 设 α 和 β 是 A 上的相容关系。

a) 复合关系 $\alpha\circ\beta$ 是 A 上的相容关系吗？

b) $\alpha\cup\beta$ 是 A 上的相容关系吗？

c) $\alpha\cap\beta$ 是 A 上的相容关系吗？

(7) 证明定理 3-11.3。

3-12 序 关 系

在一个集合上，我们常常要考虑元素的次序关系，其中很重要的一类关系称作偏序关系。

定义 3-12.1 设 A 是一个集合，如果 A 上的一个关系 R，满足自反性，反对称性和传递性，则称 R 是 A 上的一个偏序关系，并把它记为“$\preccurlyeq$”。序偶 $\langle A, \preccurlyeq\rangle$ 称作偏序集。

例题 1 在实数集 R 上，证明小于等于关系“$\leqslant$”是偏序关系。

证明 1. 对于任何实数 $a\in R$，有 $a\leqslant a$ 成立，故 R 是自反的。

2. 对任何实数 $a, b\in R$，如果 $a\leqslant b$ 且 $b\leqslant a$，则必有 $a=b$，故 R 是反对称的。

3. 如果 $a\leqslant b$，$b\leqslant c$，那么必有 $a\leqslant c$，故 R 是传递的。

因此，R 是个偏序关系。

例题 2 给定集合 $A=\{2, 3, 6, 8\}$，令“$\preccurlyeq$”$=\{\langle x, y\rangle \mid x$ 整除 $y\}$，验证“$\preccurlyeq$”是偏序关系。

解：“$\preccurlyeq$”$=\{\langle 2, 2\rangle, \langle 3, 3\rangle, \langle 6, 6\rangle, \langle 8, 8\rangle, \langle 2, 6\rangle, \langle 2, 8\rangle, \langle 3, 6\rangle\}$

写出关系矩阵和关系图如图 3-12.1 所示。

$$M_{\preccurlyeq}=\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

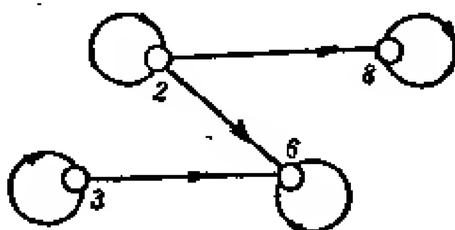


图 3-12.1

从关系矩阵和关系图可以看出“$\preccurlyeq$”是自反、反对称和传递的。

为了更清楚地描述偏序集合中元素间的层次关系，我们先介绍“盖住”的概念。

定义 3-12.2 在偏序集合 $\langle A, \preccurlyeq\rangle$ 中，如果 $x, y\in A$，$x\preccurlyeq y$，$x\neq y$ 且没有其他元素 z 满足 $x\preccurlyeq z$、$z\preccurlyeq y$，则称元素 y 盖住元素 x。并且记 $\text{COV}\,A=\{\langle x, y\rangle \mid x, y\in A; y$ 盖住 $x\}$。

例题 3 设 A 是正整数 $m=12$ 的因子的集合，并设 $\preccurlyeq$ 为整除关系，求 COV A。

解 $m=12$ 其因子集合 $A=\{1, 2, 3, 4, 6, 12\}$

“$\preccurlyeq$”$=\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 1, 4\rangle, \langle 1, 6\rangle, \langle 1, 12\rangle, \langle 2, 4\rangle, \langle 2, 6\rangle,$
$\langle 2, 12\rangle, \langle 3, 6\rangle, \langle 3, 12\rangle, \langle 4, 12\rangle, \langle 6, 12\rangle, \langle 1,1\rangle, \langle 2, 2\rangle,$
$\langle 3, 3\rangle, \langle 4, 4\rangle, \langle 6, 6\rangle, \langle 12, 12\rangle\}$

$\text{COV}\,A=\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 4\rangle, \langle 2, 6\rangle, \langle 3, 6\rangle, \langle 4, 12\rangle, \langle 6, 12\rangle\}$

对于给定偏序集 $\langle A, \preccurlyeq\rangle$，它的盖住关系是唯一的，所以可用

盖住的性质画出偏序集合图，或称哈斯图，其作图规则为：

(1) 用小圆圈代表元素。

(2) 如果 $x \preccurlyeq y$ 且 $x \neq y$，则将代表 y 的小圆圈画在代表 x 的小圆圆之上。

(3) 如果 $\langle x, y \rangle \in \mathrm{COV}\ A$，则在 x 与 y 之间用直线连接。根据这个作图规则，例题 3 中偏序集的哈斯图如图 3-12.2 所示。

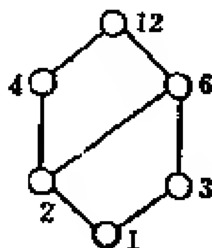


图 3-12.2

定义 3-12.3 设 $\langle A, \preccurlyeq \rangle$ 是一个偏序集合，在 A 的一个子集中，如果每两个元素都是有关系的，则称这个子集为链。在 A 的一个子集中，如果每两个元素都是无关的，则称这个子集为反链。

我们约定，若 A 的子集只有单个元素，则这个子集既是链又是反链。

例如 A 表示一个单位里所有工作人员的集合，$\preccurlyeq$ 表示领导关系，则 $\langle A, \preccurlyeq \rangle$ 为一偏序集，其中部份工作人员之间有领导关系的组成一个链。还有部份工作人员没有领导关系的组成一个反链。

例题 4 设集合 $A=\{a, b, c, d, e\}$ 上的二元关系为

$$R=\{\langle a, a\rangle, \langle a, b\rangle, \langle a, c\rangle, \langle a, d\rangle, \langle a, e\rangle, \langle b, b\rangle, \langle b, c\rangle, \langle b, e\rangle, \langle c, c\rangle, \langle c, e\rangle, \langle d, d\rangle, \langle d, e\rangle, \langle e, e\rangle\}$$

验证 $\langle A, R\rangle$ 为偏序集，画出哈斯图，举例说明链及反链。

解 写出 R 的关系矩阵

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

其关系图如图 3-12.3，从关系矩阵看到对角线都为 1，且 r_{ij} 与 r_{ji} 不同时为 1，故 R 是自反的和反对称的。

从关系图容易验证 R 是传递的，因此 R 是偏序关系。

$$\mathrm{COV}\quad A=\{\langle a, b\rangle, \langle b, c\rangle, \langle c, e\rangle, \langle a, d\rangle, \langle d, e\rangle\}$$

故哈斯图可画成图 3-12.4 所示。

集合 $\{a, b, c, e\}$，$\{a, b, c\}$，$\{b, c\}$ 和 $\{a\}$，$\{a, d, e\}$ 等都是 A 的子集也是链。

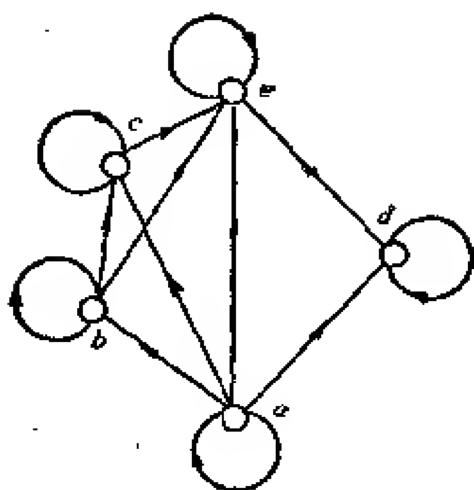


图 3-12.3

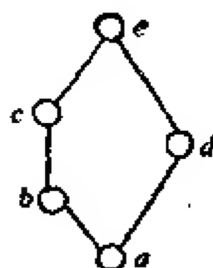


图 3-12.4

而 $\{b, d\}$, $\{c, d\}$, $\{a\}$ 等都是反链。

从例题 4 的哈斯图上容易看出，在每个链中总可从最高结点出发沿着盖住方向遍历该链中所有结点。每个反链中任两结点间均无连线。

定义 3-12.4 在偏序集 $\langle A, \preccurlyeq\rangle$ 中，如果 A 是一个链，则称 $\langle A, \preccurlyeq\rangle$ 为全序集合或称线序集合，在这种情况下，二元关系 $\preccurlyeq$ 称为全序关系或称线序关系。

全序集 $\langle A, \preccurlyeq\rangle$ 就是对任意 $x, y\in A$，或者有 $x\preccurlyeq y$ 或者有 $y\preccurlyeq x$ 成立。

例如，定义在自然数集合 N 上的"小于等于"关系"$\leqslant$"是偏序关系，且对任意 $i, j\in N$，必有：

$(i\leqslant j)$ 或 $(j\leqslant i)$ 成立，故也是全序关系。

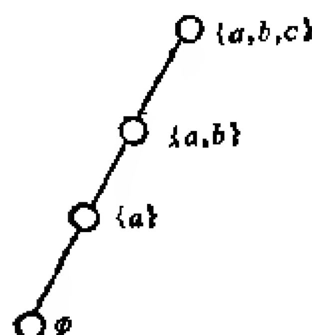


图 3-12.5

例题 5 给定 $P=\{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$ 上的包含关系 $\subseteq$，证明 $\langle P, \subseteq\rangle$ 是个全序集合。

证明 因为 $\emptyset\subseteq\{a\}\subseteq\{a, b\}\subseteq\{a, b, c\}$，故 P 中任意两元素都有包含关系。如图 3-12.5 所示。

从哈斯图中可以看到偏序集 A 中各个元素，处于不同层次的位置，下面我们讨论偏序集中具有一些特殊位置的元素。

定义 3-12.5 设 $\langle A, \preccurlyeq\rangle$ 是一个偏序集合，且 B 是 A 的子

集，对于 B 中的一个元素 b，如果 B 中没有任何元素 x，满足 $b\neq x$ 且 $b\preccurlyeq x$，则称 b 为 B 的极大元。同理，对于 $b\in B$，如果 B 中没有任何元素 x，满足 $b\neq x$ 且 $x\preccurlyeq b$，则称 b 为 B 的极小元。

例题6 设 $A=\{2, 3, 5, 7, 14, 15, 21\}$，其偏序关系

$R=\{\langle 2, 14\rangle, \langle 3, 15\rangle, \langle 3, 21\rangle, \langle 5, 15\rangle, \langle 7, 14\rangle, \langle 7, 21\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 5, 5\rangle, \langle 7, 7\rangle, \langle 14, 14\rangle, \langle 15, 15\rangle, \langle 21, 21\rangle\}$

求 $B=\{2, 7, 3, 21, 14\}$ 的极大元与极小元。

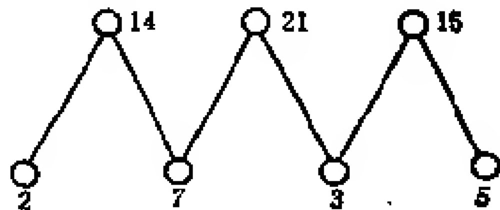


图 3-12.6

解 COV $R=\{\langle 2, 14\rangle, \langle 3, 15\rangle, \langle 3, 21\rangle, \langle 5, 15\rangle, \langle 7, 14\rangle, \langle 7, 21\rangle\}$
$\langle A, R\rangle$ 的哈斯图为图 3-12.6 所示。

故 B 的极小元集合是 $\{2, 7, 3\}$，B 的极大元集合为 $\{14, 21\}$。

从例题 6 中可以看到极大元和极小元不是唯一的。

从定义 3-12.5 中可以知道，当 $B=A$ 时，则偏序集 $\langle A, \preccurlyeq\rangle$ 的极大元即是哈斯图中最顶层的元素，其极小元是哈斯图中最低层的元素，不同的极小元素或不同的极大元素之间是无关的。

定义 3-12.6 令 $\langle A, \preccurlyeq\rangle$ 是一个偏序集，且 B 是 A 的子集，若有某个元素 $b\in B$，对于 B 中每一个元素 x 有 $x\preccurlyeq b$，则称 b 为 $\langle B, \preccurlyeq\rangle$ 的最大元。同理，若有某个元素 $b\in B$，对每一个 $x\in B$ 有 $b\preccurlyeq x$，则称 b 为 $\langle B, \preccurlyeq\rangle$ 的最小元。

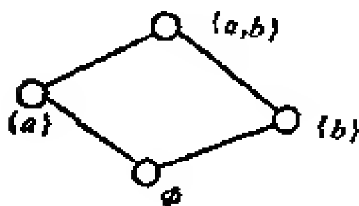


图 3-12.7

例如，考虑偏序集 $\langle\mathscr{P}(\{a, b\}), \subseteq\rangle$，其哈斯图为图 3-12.7 所示。

a) 若 $B=\{\{a\}, \emptyset\}$，则 $\{a\}$ 是 B 的最大元，$\emptyset$ 是 B 的最小元。

b) 若 $B=\{\{a\}, \{b\}\}$，则 B 没有最大元和最小元，因为 $\{a\}$ 和 $\{b\}$ 是不可比较的。

定理 3-12.1 令 $\langle A, \preccurlyeq\rangle$ 为偏序集且 $B\subseteq A$，若 B 有最大（最小）元，则必是唯一的。

证明 假定 a 和 b 两者都是 B 的最大元素，则 $a\preccurlyeq b$ 和 $b\preccurlyeq a$，从 $\preccurlyeq$ 的反对称性，得到 $a=b$。B 的最小元情况与此类似。 □

在最大(最小)元的定义中，当子集 B 与 A 相等时，B 的最大(最小)元就是偏序集 $\langle A, \preccurlyeq \rangle$ 的最大(最小)元。如例题3的图 3-12.2 中，$\langle A, \preccurlyeq \rangle$ 的最大元为 12，最小元为 1。

定义 3-12.7 设 $\langle A, \preccurlyeq \rangle$ 为一偏序集，对于 $B \subseteq A$，如有 $a \in A$，且对 B 的任意元素 x，都满足 $x \preccurlyeq a$，则称 a 为子集 B 的上界。同样地，对于 B 的任意元素 x，都满足 $a \preccurlyeq x$，则称 a 为 B 的下界。

例如，给定偏序集 $\langle A, \preccurlyeq \rangle$ 的哈斯图如图 3-12.8 所示。h, i 分别是 $B=\{a, b, c, d, e, f, g\}$ 的上界。而 f, g 分别是 $B'=\{h, i, j, k\}$ 的下界。当然，a, b, c, d, e 也可以分别是 $B'=\{h, i, j, k\}$ 的下界。但 b, c, d, e 都不是 $\{h, i, f, g\}$ 的下界。

从本例可以看到上界和下界不是唯一的。

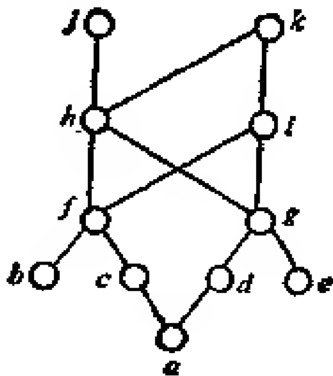


图 3-12.8

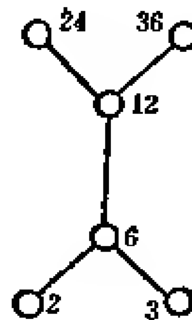


图 3-12.9

定义 3-12.8 设 $\langle A, \preccurlyeq \rangle$ 为偏序集且 $B \subseteq A$ 为一子集，a 为 B 的任一上界，若对 B 的所有上界 y 均有 $a \preccurlyeq y$，则称 a 为 B 的最小上界(上确界)，记作 LUB B。同样，若 b 为 B 的任一下界，若对 B 的所有下界 z，均有 $z \preccurlyeq b$，则称 b 为 B 的最大下界(下确界)，记作 GLB B。

例如图 3-12.8 中，a 是 $\{f, h, j, i, g\}$ 的最大下界，在图 3-12.9 中，子集 $\{2, 3, 6\}$ 的最小上界为 6，但没有最大下界。对子集 $\{12, 6\}$ 来说，最小上界为 12，最大下界是 6。

定义 3-12.9 任一偏序集合，假如它的每一个非空子集存在

最小元素，这种偏序集称为良序的。

例如，$I_n=\{1, 2, \cdots, n\}$ 及 $N=\{1, 2, 3, \cdots\}$，对于小于等于关系来说是良序集合，即 $\langle I_n, \leqslant\rangle$，$\langle N, \leqslant\rangle$ 是良序集合。

定理 3-12.2 每一个良序集合，一定是全序集合。

证明 设 $\langle A, \preccurlyeq\rangle$ 为良序集合，则对任意两个元素 $x, y\in A$ 可构成子集 $\{x, y\}$，必存在最小元素，这个最小元素不是 x 就是 y，因此一定有 $x\preccurlyeq y$ 或 $y\preccurlyeq x$。所以 $\langle A, \preccurlyeq\rangle$ 为全序集。

□

定理 3-12.3 每一个有限的全序集合，一定是良序集合。

证明 设 $A=\{a_1, a_2, \cdots, a_n\}$，令 $\langle A, \preccurlyeq\rangle$ 是全序集合，现在假定 $\langle A, \preccurlyeq\rangle$ 不是良序集合，那么必存在一个非空子集 $B\subseteq A$，在 B 中不存在最小元素，由于 B 是一个有限集合，故一定可以找出两个元素 x 与 y 是无关的，由于 $\langle A, \preccurlyeq\rangle$ 是全序集，$x, y\in A$，所以 x, y 必有关系，得出矛盾，故 $\langle A, \preccurlyeq\rangle$ 必是良序集合。 □

上述结论对于无限的全序集合不一定成立。

例如，大于零小于 1 的全部实数，按大小次序关系是一个全序集合，但不是良序集合，因为集合本身就不存在最小元素。

3-12 习题

(1) 设集合为 $\{3, 5, 15\}$，$\{1, 2, 3, 6, 12\}$，$\{3, 9, 27, 54\}$，偏序关系为整除，画出这些集合的偏序关系图，并指出哪些是全序关系。

(2) 设 R 是 A 上的二元关系，如果 R 是传递的和反自反的，称 R 是拟序关系。证明：

a) 如果 R 是 A 上拟序关系，则 $r(R)=R\cup I_A$ 是偏序关系。

b) 如果 R 是一偏序关系，则 $R-I_A$ 是一拟序关系。

(3) 设 R 是集合 S 上的关系，S' 是 S 的子集，定义 S' 上的关系 R' 如下：

$$R'=R\cap(S'\times S')$$

确定下述每一断言是真还是假。

a) 如果 R 在 S 上是传递的，那么 R' 在 S' 上是传递的。

b) 如果 R 是 S 上的偏序关系，那么 R' 是 S' 上的偏序关系。

c) 如果 R 是 S 上的拟序关系，那么 R' 是 S' 上的拟序关系。

d) 如果 R 是 S 上的线序关系，那么 R' 是 S' 上的线序关系。

e) 如果 R 是 S 上的良序关系，那么 R' 是 S' 上的良序关系。

(4) 找出在集合 $\{0, 1, 2, 3\}$ 上包含序偶 $\langle 0, 3\rangle$ 和 $\langle 2, 1\rangle$ 的线序关系。

(5) 构造下述集合的例子。

a) 非空线序集，其中某些子集没有最小元素。

b) 非空偏序集，它不是线序集，其中某些子集没有最大元。

c) 一偏序集有一子集，它存在一最大下界，但没有最小元素。

d) 一偏序集有一子集，它存在一上界但没有最小上界。

(6) 设集合 $P=\{x_1, x_2, x_3, x_4, x_5\}$ 上的偏序关系如图 3-12.10 所示。找出 P 的最大元素，最小元素，极小元素，极大元素。找出子集 $\{x_2, x_3, x_4\}$，$\{x_3, x_4, x_5\}$ 和 $\{x_1, x_2, x_3\}$ 的上界、下界，上确界、下确界。

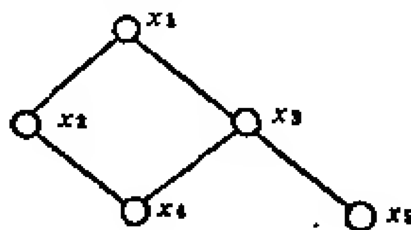


图 3-12.10

(7) 图 3-12.11 给出了集合 $\{1, 2, 3, 4\}$ 上的四个偏序关系图，画出它们的哈斯图，并说明哪一个是全序关系，哪一个是良序关系。

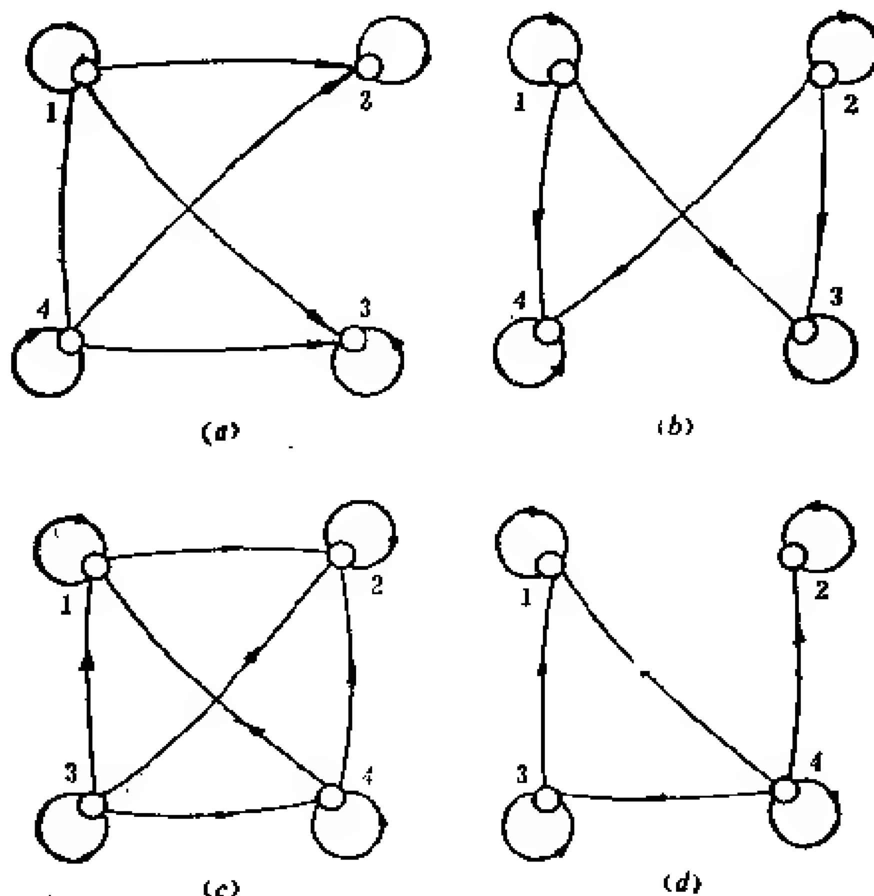


图 3-12.11

第四章 函　数

函数是一个基本的数学概念，在通常的函数定义中，$y=f(x)$是在实数集合上讨论，我们这里把函数概念予以推广，把函数看作是一种特殊的关系。例如，计算机中把输入、输出间的关系看成是一种函数；类似地，在开关理论、自动机理论和可计算性理论等领域中，函数都有着极其广泛的应用。

4-1 函数的概念

定义4-1.1 设X和Y是任何两个集合，而f是X到Y的一个关系，如果对于每一个$x\in X$，有唯一的$y\in Y$，使得$\langle x,y\rangle\in f$，称关系f为函数，记作：

$$f\colon X\to Y \text{ 或 } X\xrightarrow{f}Y$$

假如$\langle x, y\rangle\in f$，则x称为自变元，y称为在f作用下x的象，$\langle x, y\rangle\in f$亦可记作$y=f(x)$，且记

$$f(X)=\{f(x)\mid x\in X\}$$

从函数的定义可以知道它与关系有别于如下两点。

a. 函数的定义域是X，而不能是X的某个真子集。

b. 一个$x\in X$只能对应于唯一的一个y。即如果$f(x)=y$且$f(x)=z$，那么，$y=z$。从X到Y的函数往往也叫做从X到Y的映射。

在$\langle x, y\rangle\in f$中，f的前域就是函数$y=f(x)$的定义域记作$\mathrm{dom}f=X$，f的值域$\mathrm{ran}\,f\subseteq Y$，有时也记为$R_f$，即

$$R_f=\{y\mid(\exists x)(x\in X)\land(y=f(x))\}$$

集合Y称为f的共域，$\mathrm{ran}\,f$亦称为函数的象集合。

例1 设$X=\{1, 5, p, 张明\}$，$Y=\{2, q, 7, 9, G\}$

$$f=\{\langle 1, 2\rangle, \langle 5, q\rangle, \langle p, 7\rangle, \langle \text{张明}, G\rangle\}$$

即 $f(1)=2,\ f(5)=q,\ f(p)=7,\ f(\text{张明})=G$，故

$$\mathrm{dom}\ f=X,\ R_f=\{2, q, 7, G\}$$

例 2 设 A 是房子的集合，B 是不同颜色油漆的集合，那么，油漆房子的一种颜色的分配方案是 A 到 B 的一个函数，即

$$A \xrightarrow{f} B$$

其中 $\mathrm{dom}\ f=A$，$\mathrm{ran}\ f\subseteq B$。

例 3 判别下列关系中哪个能构成函数。

a. $f=\{\langle x_1, x_2\rangle \mid x_1, x_2\in N, \text{且}\ x_1+x_2<10\}$

因为 x_1 不能取定义域中所有的值，且 x_1 对应很多 x_2，故这个关系不能构成函数。

b. $f=\{\langle y_1, y_2\rangle \mid y_1, y_2\in R, y_2^2=y_1\}$

因为一个 y_1 对应两个 y_2，故也不是函数。

c. $f=\{\langle x_1, x_2\rangle \mid x_1, x_2\in N, x_2\ \text{为小于}\ x_1\ \text{的素数个数}\}$

能够成为函数。

因为函数是序偶的集合，故两个函数相等可用集合相等的概念予以定义。

定义 4-1.2 设函数 $f: A\to B$, $g: C\to D$，如果 $A=C$，$B=D$，且对于所有 $x\in A$ 和 $x\in C$ 有 $f(x)=g(x)$，则称函数 f 和 g 相等，记作 $f=g$。

从函数的定义可以知道，$X\times Y$ 的子集并不能都成为 X 到 Y 的函数。

例如，设 $X=\{a, b, c\}$，$Y=\{0, 1\}$，$X\times Y=\{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 0\rangle, \langle a, 1\rangle, \langle b, 1\rangle\langle c, 1\rangle\}$，$X\times Y$ 有 2^6 个可能的子集，但其中只有 2^3 个子集定义为从 X 到 Y 的函数。

$$f_0=\{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 0\rangle\}$$

$$f_1=\{\langle a, 0\rangle, \langle b, 0\rangle, \langle c, 1\rangle\}$$

$$f_2=\{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 0\rangle\}$$

$$f_3=\{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 1\rangle\}$$

$$f_4=\{\langle a,\ 1\rangle,\langle b,\ 0\rangle,\langle c,\ 0\rangle\}$$
$$f_5=\{\langle a,\ 1\rangle,\langle b,\ 0\rangle,\langle c,\ 1\rangle\}$$
$$f_6=\{\langle a,\ 1\rangle,\langle b,\ 1\rangle,\langle c,\ 0\rangle\}$$
$$f_7=\{\langle a,\ 1\rangle,\langle b,\ 1\rangle,\langle c,\ 1\rangle\}$$

设 X 和 Y 都为有限集，分别有 m 个和 n 个不同元素，由于从 X 到 Y 任意一个函数的定义域是 X，在这些函数中每一个恰有 m 个序偶。另外任何元素 $x\in X$，可以有 Y 的 n 个元素中的任何一个作为它的象，故共有 n^m 个不同的函数。在上例中 $n=2$，$m=3$，故应有 2^3 个不同的函数。今后我们用符号 Y^X 表示从 X 到 Y 的所有函数的集合，甚至当 X 和 Y 是无限集时，也用这个符号。

下面，我们讨论函数的几类特殊情况。

定义 4-1.3 对于 $X\xrightarrow{f}Y$ 的映射中，如果 $\mathrm{ran}\,f=Y$，即 Y 的每一个元素是 X 中一个或多个元素的象点，则称这个映射为满射(或到上映射)。

设 f: $X\to Y$ 是满射，即是对于任意 $y\in Y$，必存在 $x\in X$ 使得 $f(x)=y$ 成立。

例如，$A=\{a,\ b,\ c,\ d\}$，$B=\{1,\ 2,\ 3\}$，如果 $A\xrightarrow{f}B$ 为：

$$f(a)=1,\ f(b)=1,\ f(c)=3,\ f(d)=2$$

则 f 是满射的。

定义 4-1.4 从 X 到 Y 的映射中，X 中没有两个元素有相同的象，则称这个映射为入射(或一对一映射)。设 f: $X\to Y$ 是入射，即是对于任意 $x_1,\ x_2\in X$，如果

$$x_1\neq x_2\Rightarrow f(x_1)\neq f(x_2)$$

或者

$$f(x_1)=f(x_2)\Rightarrow x_1=x_2$$

例如，函数 f: $\{a,\ b\}\to\{2,\ 4,\ 6\}$ 为 $f(a)=2$，$f(b)=6$，则这个函数是入射，但不是满射。

定义 4-1.5 从 X 到 Y 的一个映射，若既是满射又是入射

的，则称这个映射是双射的。

例如，令$[a, b]$表示实数的闭区间，即 $[a, b]=\{x|a\leqslant x\leqslant b\}$，令$f: [0, 1]\to[a, b]$，这里$f(x)=(b-a)x+a$，这个函数是双射的。

例如在图 4-1.1 中，(a)，(c)是满射，(b)，(c)是入射，(c)是双射。

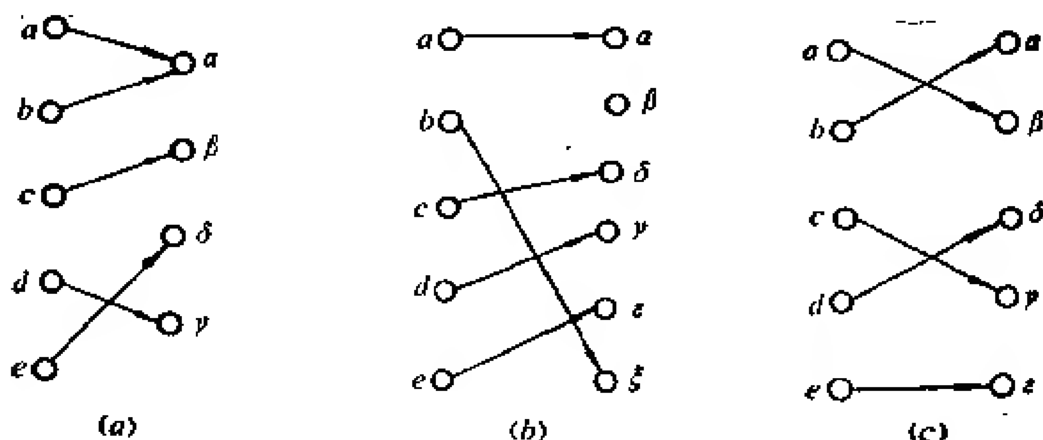


图 4-1.1

映射的概念在日常生活中也有很多应用。如设 X 是工人的集合，Y 表示工作的集合，从 X 到 Y 的满射是工人做工作的一种分配方案，使每项工作至少分配有一个工人。从 X 到 Y 的入射，也是一种分配方案，使得没有两个工人做同一项工作。从 X 到 Y 的双射，同样是一种分配方案，使每一项工作都分配有工人，而且没有两个工人分配相同的工作。

定理 4-1.1 令 X 和 Y 为有限集，若 X 和 Y 的元素个数相同，即$|X|=|Y|$，则$f: X\to Y$ 是入射的，当且仅当它是一个满射。

证明 a. 若 f 是入射，则 $|X|=|f(X)|$，因为 $|f(X)|=|Y|$，从 f 的定义我们有 $f(X)\subseteq Y$，而$|f(X)|=|Y|$，又因为$|Y|$ 是有限的，故 $f(X)=Y$；因此 f 是一个入射推出 f 是满射。

b. 若 f 是一个满射，根据满射定义 $f(X)=Y$，于是 $|X|=|Y|=|f(X)|$。因为$|X|=|f(X)|$和$|X|$是有限的，故 f 是一个入射，因此 f 是满射推出 f 是一个入射。 □

这个定理必须在有限集情况下才能成立，在无限集上不一定有效，如 $f: I \to I$，这里 $f(x)=2x$，在这种情况下整数映射到偶整数，显然这是一个入射，但不是满射。

4-1 习题

(1) 下列函数中哪些是入射的，满射的或双射的。

(a) $f: I \to I,\ f(j)=j(\text{mod } 3)$

(b) $f: N \to N,\quad f(j)=\begin{cases}1 & j\text{是奇数}\\ 0 & j\text{是偶数}\end{cases}$

(c) $f: N \to \{0, 1\},\ f(j)=\begin{cases}0 & j\text{是奇数}\\ 1 & j\text{是偶数}\end{cases}$

(d) $f: I \to N \quad f(i)=|2i|+1$

(e) $f: R \to R \quad f(r)=2r-15$

(2) 令 $f: A \to B$，这里 $C \subseteq A$，证明

$$f(A)-f(C) \subseteq f(A-C)$$

(3) 假设 f 和 g 是函数，且有 $f \subseteq g$ 和 $\text{dom } g \subseteq \text{dom } f$，证明

$$f=g$$

(4) 假设 f 和 g 是函数，证明 $f \cap g$ 也是函数。

(5) 假定 X 和 Y 是有穷集合，找出从 X 到 Y 存在入射的必要条件是什么？

(6) 设 A 和 B 是有穷集合，有多少不同入射函数和多少不同的双射函数。

(7) 试证明 $f(A \cup B)=f(A) \cup f(B)$

$f(A \cap B) \subseteq f(A) \cap f(B)$

(8) 假设 $f: A \to B$ 并定义一个函数 $G: B \to \mathscr{P}(A)$，对于 $b \in B$

$$G(b)=\{x \in A \mid f(x)=b\}$$

证明，如果 f 是 A 到 B 的满映射，则 G 是入射的；其逆成立吗？

4-2 逆函数和复合函数

在关系的定义中曾提到，从 X 到 Y 的关系 R，其逆关系 R^c 是 Y 到 X 的关系。$\langle y, x\rangle \in R^c \Leftrightarrow \langle x, y\rangle \in R$。但是对于函数就不能用简单的交换序偶的元素而得到逆函数，这是因为若有函数

$f: X \to Y$，但 f 的值域 R_f 可能只是 y 的一个真子集，即 $R_f \subset Y$，因为 $\text{dom}\, f^c = R_f \subset Y$，这不符函数定义域的要求。此外，若 $X \xrightarrow{f} Y$ 的映射是一个多一对应，即有 $\langle x_1, y\rangle \in f$，$\langle x_2, y\rangle \in f$，其逆关系将有 $\langle y, x_1\rangle \in f^c$，$\langle y, x_2\rangle \in f^c$，这就违反函数值唯一性的要求。为此，我们对函数求逆需规定一些条件。

定理 4-2.1 设 $f: X \to Y$ 是一双射函数，那么 f^c 是 $Y \to X$ 的双射函数。

证明 设 $f = \{\langle x, y\rangle \mid x \in X \land y \in Y \land f(x) = y\}$

$$f^c = \{\langle y, x\rangle \mid \langle x, y\rangle \in f\}$$

因为 f 是满射的，故每一 $y \in Y$ 必存在 $\langle x, y\rangle \in f$，因此必有 $\langle y, x\rangle \in f^c$，即 f^c 的前域为 Y。又因为 f 是入射，对每一个 $y \in Y$ 恰有一个 $x \in X$，使 $\langle x, y\rangle \in f$，因此仅有一个 $x \in X$，使 $\langle y, x\rangle \in f^c$，即 y 对应唯一的 x，故 f^c 是函数。

又因 $\text{ran}\, f^c = \text{dom}\, f = X$，故 f^c 是满射。又若 $y_1 \neq y_2$ 有

$$f^c(y_1) = f^c(y_2)$$

因为 $f^c(y_1) = x_1$，$f^c(y_2) = x_2$，即 $x_1 = x_2$，故 $f(x_1) = f(x_2)$，即 $y_1 = y_2$，得出矛盾。因此 f^c 是一个双射函数。 □

定义 4-2.1 设 $f: X \to Y$ 是一双射函数，称 $Y \to X$ 的双射函数 f^c 为 f 的逆函数，记作 f^{-1}。

例如，设 $A = \{1, 2, 3\}$，$B = \{a, b, c\}$，$f: A \to B$ 为

$$f = \{\langle 1, a\rangle, \langle 2, c\rangle, \langle 3, b\rangle\}$$

则 $$f^{-1} = \{\langle a, 1\rangle, \langle c, 2\rangle, \langle b, 3\rangle\}$$

若 $$f = \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, b\rangle\}$$

则 f 的逆关系

$$f^c = \{\langle a, 1\rangle, \langle b, 2\rangle, \langle b, 3\rangle\}$$

就不是一个函数。

定义 4-2.2 设函数 $f: X \to Y$，$g: W \to Z$，若 $f(X) \subseteq W$，则 $g \circ f = \{\langle x, z\rangle \mid x \in X \land z \in Z \land (\exists y)(y \in Y \land y = f(x) \land z = g(y))\}$，称 g 在函数 f 的左边可复合。

定理4-2.2 两个函数的复合是一个函数。

证明 设 $g: W \to Z$, $f: X \to Y$ 为左复合，即 $f(X) \subseteq W$。

a) 对于任意 $x \in X$，因为 f 为函数，故必有唯一的序偶 $\langle x, y\rangle$ 使 $y = f(x)$ 成立，而 $f(x) \in f(X)$ 即 $f(x) \in W$，又因为 g 是函数，故必有唯一序偶 $\langle y, z\rangle$ 使 $z = g(y)$ 成立，根据复合定义，$\langle x, z\rangle \in g \circ f$，即 X 中每个 x 对应 Z 中某个 z。

b) 假定 $g \circ f$ 中包含序偶 $\langle x, z_1\rangle$ 和 $\langle x, z_2\rangle$ 且 $z_1 \neq z_2$，这样在 Y 中必存在 y_1 和 y_2，使得在 f 中有 $\langle x, y_1\rangle$ 和 $\langle x, y_2\rangle$ 在 g 中有 $\langle y_1, z_1\rangle$ 和 $\langle y_2, z_2\rangle$。因为 f 是一个函数，故 $y_1 = y_2$。于是 g 中有 $\langle y, z_1\rangle$ 和 $\langle y, z_2\rangle$，但 g 是一个函数，故 $z_1 = z_2$，即每个 $x \in X$ 只能有唯一的 $\langle x, z\rangle \in g \circ f$。

由 a), b) 可知 $g \circ f$ 是一个函数。 □

在定义 4-2.2 中，当 $W = Y$ 时，则函数 $f: X \to Y$, $g: Y \to Z$。

$$g \circ f = \{\langle x, z\rangle \mid x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge y = f(x) \wedge z = g(y))\}$$

称为复合函数，或称 $g \circ f$ 为 g 对 f 的左复合。

注意：在上述定义中，假定 $\operatorname{ran} f \subseteq \operatorname{dom} g$，如果不满足这个条件，则定义 $g \circ f$ 为空。

根据复合函数的定义，显然有 $g \circ f(x) = g(f(x))$。

例题 1 设 $X = \{1, 2, 3\}$, $Y = \{p, q\}$, $Z = \{a, b\}$, $f = \{\langle 1, p\rangle, \langle 2, p\rangle, \langle 3, q\rangle\}$, $g = \{\langle p, b\rangle, \langle q, b\rangle\}$ 求 $g \circ f$。

解 $g \circ f = \{\langle 1, b\rangle, \langle 2, b\rangle, \langle 3, b\rangle\}$

定理4-2.3 令 $g \circ f$ 是一个复合函数。

a) 若 g 和 f 是满射的，则 $g \circ f$ 是满射的。

b) 若 g 和 f 是入射的，则 $g \circ f$ 是入射的。

c) 若 g 和 f 是双射的，则 $g \circ f$ 是双射的。

证明 a) 设 $f: X \to Y$, $g: Y \to Z$，令 z 为 Z 的任意一个元素，因 g 是满射，故必有某个元素 $y \in Y$ 使得 $g(y) = z$，又因为 f 是满射，故必有某个元素 $x \in X$，使得 $f(x) = y$，故

$$g \circ f(x) = g(f(x)) = g(y) = z$$

因此，$R_{g\circ f}=Z$，$g\circ f$ 是满射的。

b) 令 x_1，x_2 为 X 的元素，假定 $x_1\neq x_2$，因为 f 是入射的，故 $f(x_1)\neq f_1(x_2)$。又因 g 是入射的且 $f(x_1)\neq f(x_2)$，故 $g(f(x_1))\neq g(f(x_2))$，于是 $x_1\neq x_2\Rightarrow g\circ f(x_1)\neq g\circ f(x_2)$，因此，$g\circ f$ 是入射的。

c) 因为 g 和 f 是双射，故根据 a) 与 b)，$g\circ f$ 为满射和入射的，即 $g\circ f$ 是双射的。 □

由于函数的复合仍然是一个函数，故可求三个函数的复合。

例题 2 设 R 为实数集合，对 $x\in R$ 有 $f(x)=x+2$，$g(x)=x-2$，$h(x)=3x$。求 $g\circ f$ 与 $h\circ(g\circ f)$。

解
$$g\circ f=\{\langle x, x\rangle\mid x\in R\}$$
$$h\circ(g\circ f)=\{\langle x, 3x\rangle\mid x\in R\}$$

一般地，我们有 $h\circ(g\circ f)=(h\circ g)\circ f$。函数的复合是可结合的，故我们可以去掉上式中的括号。它的证明如图 4-2.1 所示。

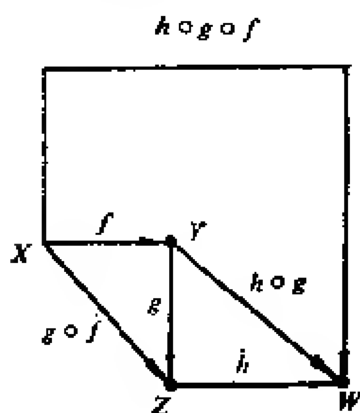


图 4-2.1

定义 4-2.3 函数 $f: X\rightarrow Y$ 叫做常函数，如果存在某个 $y_0\in Y$，对于每个 $x\in X$ 都有 $f(x)=y_0$，即 $f(X)=\{y_0\}$。

定义 4-2.4 如果
$$I_X=\{\langle x, x\rangle\mid x\in X\}$$
则称函数 I_X: $X\rightarrow X$ 为恒等函数。

定理 4-2.4 设函数 f: $X\rightarrow Y$，则
$$f=f\circ I_X=I_Y\circ f$$
这个定理的证明可以由定义直接得到。 □

定理 4-2.5 如果函数 f: $X\rightarrow Y$ 有逆函数 f^{-1}: $Y\rightarrow X$，则
$$f^{-1}\circ f=I_X$$
且
$$f\circ f^{-1}=I_Y$$

证明 a) $f^{-1}\circ f$ 与 I_X 的定义域均是 X。

b) 因为 f 为一一对应的函数，故 f^{-1} 也是一一对应的函数。若 f: $x\rightarrow f(x)$ 则 $f^{-1}(f(x))=x$，由 a)，b) 得 $f^{-1}\circ f=I_X$，故 $x\in X\Rightarrow(f^{-1}\circ f)(x)=f^{-1}(f(x))=x$。 □

例题3 令f: $\{0, 1, 2\} \to \{a, b, c\}$，其定义如图4-2.2(a)所示，求$f^{-1}\circ f$和$f\circ f^{-1}$。

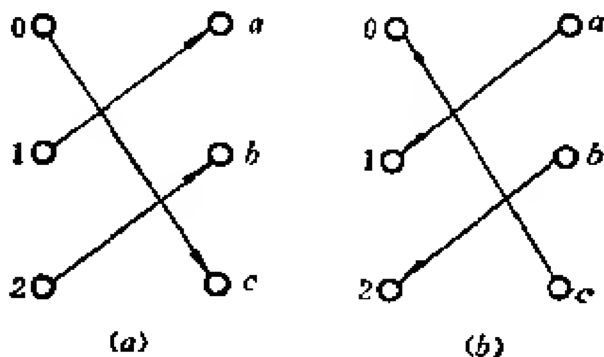


图 4-2.2

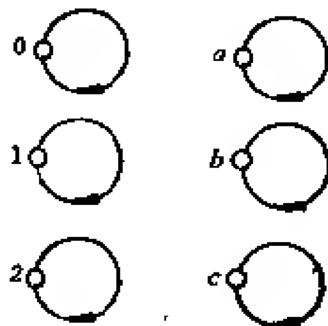


图 4-2.3

解 $f^{-1}\circ f$和$f\circ f^{-1}$可表示为如图4-2.3所示。

定理4-2.6 若f: $X \to Y$是一一对应的函数，则$(f^{-1})^{-1}=f$。

证明 a) 因f: $X\to Y$是一一对应的，故f^{-1}: $Y\to X$也是一一对应的函数，因此$(f^{-1})^{-1}$: $X\to Y$又为一一对应，显然

$$\mathrm{dom}\, f=\mathrm{dom}(f^{-1})^{-1}=X$$

b) $x\in X \Rightarrow f: x\to f(x) \Rightarrow f^{-1}: f(x)\to x \Rightarrow (f^{-1})^{-1}: x\to f(x)$。

由a)，b)可知

$$(f^{-1})^{-1}=f$$ □

定理4-2.7 若f: $X\to Y$，g: $Y\to Z$均为一一对应函数，则$(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

证明 a) 因f: $X\to Y$，g: $Y\to Z$均为一一对应函数，故f^{-1}和g^{-1}均存在，且f^{-1}: $Y\to X$，g^{-1}: $Z\to Y$，所以$f^{-1}\circ g^{-1}$: $Z\to X$。

根据定理4-2.2，$g\circ f$: $X\to Z$是双射的，故$(g\circ f)^{-1}$存在且$(g\circ f)^{-1}$: $Z\to X$。

$$\mathrm{dom}(f^{-1}\circ g^{-1})=\mathrm{dom}(g\circ f)^{-1}=Z$$

b) 对任意$z\in Z \Rightarrow$ 存在唯一$y\in Y$，使得$g(y)=z \Rightarrow$ 存在唯一$x\in X$，使得$f(x)=y$，故

$$(f^{-1}\circ g^{-1})(z)=f^{-1}(g^{-1}(z))=f^{-1}(y)=x$$

但 $$(g\circ f)(x)=g(f(x))=g(y)=z$$

故 $$(g\circ f)^{-1}(z)=x$$

因此对任一 $z\in Z$ 有：

$$(g\circ f)^{-1}(z)=(f^{-1}\circ g^{-1})(z)$$

由 a)，b)可知

$$f^{-1}\circ g^{-1}=(g\circ f)^{-1}$$ □

4-2 习题

(1) 设 $X=\{1, 2, 3, 4\}$，确定出这样的函数 f: $X\to X$ 使得 $f\neq I_x$，并且是入射的，求出 $f\circ f=f^2$，$f^3=f\circ f^2$，f^{-1} 和 $f\circ f^{-1}$。是否能够找出另外一个入射函数 g: $X\to X$ 使得 $g\neq I_x$ 但是 $g\circ g=I_x$。

(2) 设 f: $A\to B$，$B'\subseteq B$，$A'\subseteq A$，证明

a) $f(f^{-1}(B'))\subseteq B'$

b) 如果 f 是满射的，那末 $f(f^{-1}(B'))=B'$

c) $f^{-1}(f(A'))\supseteq A'$

d) 如果 f 是入射的，那末 $f^{-1}(f(A'))=A'$

(3) 设 $f\circ g$ 是复合函数，

a) 如果 $f\circ g$ 是满射的，那末 f 是满射的。

b) 如果 $f\circ g$ 是入射的，那末 g 是入射的。

c) 如果 $f\circ g$ 是双射的，那末 f 是满射的而 g 是入射的。

(4) 试证 若 f: $A\to B$，g: $B\to A$，且 $g\circ f=I_A$，$f\circ g=I_B$，则 $g=f^{-1}$，且 $f=g^{-1}$。

(5) 证明 若 $(g\circ f)^{-1}$ 是一个函数，则 f 和 g 是入射不一定成立。

(6) 一个函数 g: $S\to T$ 是称作函数 f: $T\to S$ 的左逆，若对每个 $t\in T$，$g(f(t))=t$，若 g 是 f 的左逆，则 f 是 g 的右逆。

a) f: $T\to S$ 有一个左逆，当且仅当它是入射的。

b) f: $T\to S$ 有一个右逆，当且仅当它是满射的。

c) 若 g: $S\to T$ 是 f: $T\to S$ 的左逆和右逆，则 f 是一个双射，且 $g=f^{-1}$。

*4-3 特征函数与模糊子集

有些函数与集合之间可以建立一些特殊的联系，借助于这些函数，可对集合进行运算，并能以此推广表达模糊集合的概念。

定义 4-3.1 令 E 是全集，A 是 E 的子集，$A\subseteq E$，由

$$\psi_A(x)=\begin{cases}1 & 如果\ x\in A\\ 0 & 其他\end{cases}$$

定义的函数 ψ_A: $E\to\{0, 1\}$，称为集合 A 的特征函数。

例如，E 是某班级全体学生的集合，A 是全体女学生的集合，则 ψ_A 为女学生的特征函数。

设 A 和 B 是全集 E 的任何两个子集，对于所有 $x\in E$，特征函数有如下一些性质。

$$\psi_A(x)=0\Leftrightarrow A=\phi \tag{1}$$

$$\psi_A(x)=1\Leftrightarrow A=E \tag{2}$$

$$\psi_A(x)\leqslant\psi_B(x)\Leftrightarrow A\subseteq B \tag{3}$$

$$\psi_A(x)=\psi_B(x)\Leftrightarrow A=B \tag{4}$$

$$\psi_{A\cap B}(x)=\psi_A(x)*\psi_B(x) \tag{5}$$

$$\psi_{A\cup B}(x)=\psi_A(x)+\psi_B(x)-\psi_{A\cap B}(x) \tag{6}$$

$$\psi_{\sim A}(x)=1-\psi_A(x) \tag{7}$$

$$\psi_{A-B}(x)=\psi_{A\cap\sim B}=\psi_A(x)-\psi_{A\cap B}(x) \tag{8}$$

其中特征函数两的运算 +，-，* 就是通常的算术运算 +，-，×。用于集合间的相等，就是通常所定义的集合相等。

上述几个性质可以从特征函数的定义给予证明。如(5)式可证明如下：

设 $x\in A\cap B$，因为 $x\in A\cap B\Leftrightarrow x\in A\wedge x\in B$，因此

$$\psi_A(x)=1,\ \psi_B(x)=1$$

所以
$$\psi_{A\cap B}(x)=\psi_A(x)*\psi_B(x)=1$$

设 $x\notin A\cap B$，因为

$$x\notin A\cap B\Leftrightarrow x\notin A\vee x\notin B$$

因此
$$\psi_A(x)=0$$

或
$$\psi_B(x)=0$$

$$\psi_{A\cap B}(x)=\psi_A(x)*\psi_B(x)=0$$

应用特征函数的一些性质，也可以证明一些集合恒等式。

例题1　证明　$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

解

$$\begin{aligned}\psi_{A\cap(B\cup C)}(x)&=\psi_A(x)*\psi_{B\cup C}(x)\\&=\psi_A(x)*(\psi_B(x)+\psi_C(x)-\psi_{B\cap C}(x))\\&=\psi_A(x)*\psi_B(x)+\psi_A(x)*\psi_C(x)-\psi_A(x)*\psi_{B\cap C}(x)\\&=\psi_{A\cap B}(x)+\psi_{A\cap C}(x)-\psi_{A\cap B\cap C}(x)\\&=\psi_{A\cap B}(x)+\psi_{A\cap C}(x)-\psi_{(A\cap B)\cap(A\cap C)}(x)\\&=\psi_{(A\cap B)\cup(A\cap C)}(x)\end{aligned}$$

例题2　设 $E=\{a, b, c\}$，E 的子集是：$\emptyset$，$\{a\}$，$\{b\}$，$\{c\}$，$\{a, b\}$，$\{a, c\}$，$\{b, c\}$ 和 $\{a, b, c\}$。试给出 E 的所有子集的特征函数且建立特征函数与二进制之间的对应关系。

解　E 的任何子集 A 的特征函数的值由表 4-3.1 列出。

表　4-3.1

x \ $\psi_A(x)$	A							
	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a, b, c\}$
a	0	1	0	0	1	1	0	1
b	0	0	1	0	1	0	1	1
c	0	0	0	0	0	1	1	1

如果规定元素的次序为 a, b, c，则每个子集 A 的特征函数与一个三位二进制数相对应。如 $\psi_{\{a,c\}}(x)\leftrightarrow 101$。令 $B=\{000, 001, 010, 011, 100, 101, 110, 111\}$，那么表 4-3.1 亦可以看作从 E 的幂集到 B 的一个双射。

对于特征函数进行推广可以导出模糊子集的概念。

设 $E=\{x_1, x_2, \cdots, x_n\}$，我们可以将 E 的任一子集 A 表示为：

$$\underset{\sim}{A}:\{\langle x_1, \psi_A(x_1)\rangle, \langle x_2, \psi_A(x_2)\rangle, \cdots, \langle x_n, \psi_A(x_n)\rangle\}$$

当　　$\psi_A(x_i)=1$ 时　$x_i\in A$

　　　$\psi_A(x_i)=0$ 时　$x_i\notin A$

如果我们将 $\psi_A(x_i)$ 的取值范围不局限于 0 和 1，而是取 0 和 1 之间的任何数，例如：

$$\underset{\sim}{A}^*:\{\langle x_1, 0.2\rangle, \langle x_2, 0\rangle, \langle x_3, 0.3\rangle, \langle x_4, 1\rangle, \langle x_5, 0.8\rangle\}$$

那么，对 A^* 可以作如下理解：它表示 x_1 是少量地属于 A^*，x_2 是

不属于 A^*，x_3 也是少量地属于 A^*（但是比 x_1 稍多），x_4 是必定属于 A^*，x_5 则基本上属于 A^*。这样的一个集合 $\underset{\sim}{A}^*$ 就是一个模糊子集，其中 0.2, 0.3, 0.8, …分别称为该集合中对应元素的隶属程度。

定义 4-3.2 给定论域 E，指定 E 上的一个模糊子集 $\underset{\sim}{A}$ 是指对任意 $x\in E$ 都有一个隶属程度 $\mu=\psi_{\underset{\sim}{A}}(x)$ $(0\leqslant\mu\leqslant1)$ 与它对应，称 $\psi_{\underset{\sim}{A}}(x)$ 为 $\underset{\sim}{A}$ 的隶属函数。

从模糊子集的定义可以看出，当 $\psi_{\underset{\sim}{A}}(x)$ 只取 0，1 两值时，$\underset{\sim}{A}$ 便成为普通子集。

例 1 如图 4-3.1 所示，给定几个物体的集合。

$$U=\{a,\ b,\ c,\ d,\ e\}$$

对每个元素指定一个隶属程度。

$$\psi_{\underset{\sim}{A}}(a)=1,$$
$$\psi_{\underset{\sim}{A}}(b)=0.9$$
$$\psi_{\underset{\sim}{A}}(c)=0.4$$
$$\psi_{\underset{\sim}{A}}(d)=0.2,$$
$$\psi_{\underset{\sim}{A}}(e)=0$$

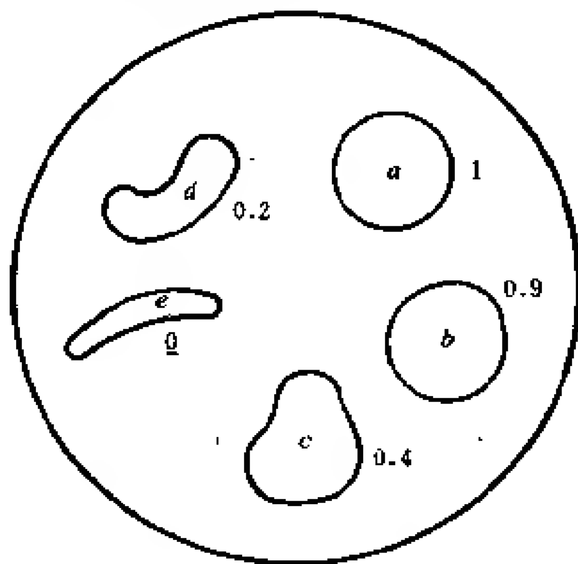


图 4-3.1

于是可确定 U 的模糊子集 $\underset{\sim}{A}$，若 $\underset{\sim}{A}$ 表示"圆块"这个概念，则可记模糊子集

$$\underset{\sim}{A}=1/a+0.9/b+0.4/c+0.2/d+0/e$$

注意在这种记法中，上式右端不是分式求和，该式中分母表示元素，分子表示隶属程度。

例 2 以年龄作论域，取 $U=[0,\ 100]$，"年老"与"年轻"这样两个模糊概念可以分别用两个模糊子集 $\underset{\sim}{O}$ 与 $\underset{\sim}{Y}$ 来表示，它们的隶属函数可分别定义为：

$$\psi_{\underset{\sim}{O}}(u)=\begin{cases}0 & (0\leqslant u\leqslant50)\\ \left[1+\left(\dfrac{u-50}{5}\right)^{-2}\right]^{-1} & (50<u\leqslant100)\end{cases}$$

$$\psi_Y(u)=\begin{cases}1 & (0\leqslant u\leqslant 25)\\ \left[1+\left(\frac{u-25}{5}\right)^2\right]^{-1} & (25<u\leqslant 100)\end{cases}$$

从这两个例子，可以看到在论域上确定模糊子集，主要的是需定出隶属函数，即是要确定恰当的表示模糊特征的那个特征函数(参见图 4-3.2)。

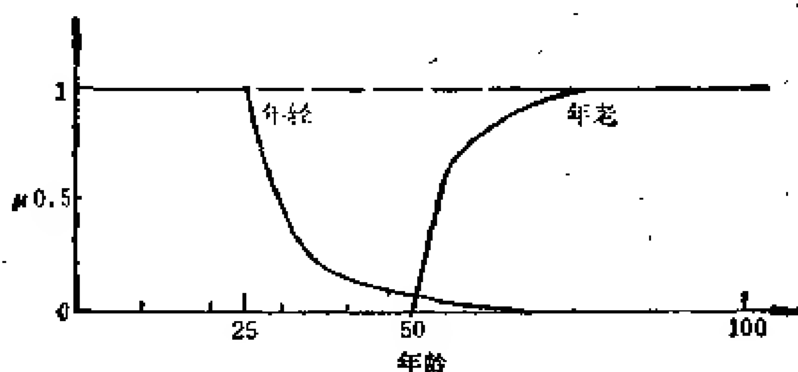


图 4-3.2

有关模糊子集的其他理论，这里就不再讨论了。

4-3 习题

(1) 试证明，对于所有的 $x\in E$

a) $\psi_A(x)\leqslant\psi_B(x)$ 当且仅当 $A\subseteq B$

b) $\psi_{A\cap B}(x)=\min(\psi_A(x),\ \psi_B(x))$

c) $\psi_{A\cup B}(x)=\max(\psi_A(x),\ \psi_B(x))$

d) $\psi_{A-B}(x)=\psi_A(x)-\psi_{A\cap B}(x)$

(2) 设 $E=[0,1]$, $A=\left[\frac{1}{2},\ 1\right]$ 画出 ψ_A 的图。

(3) 设 $S=(A\cap B)\cup(\sim A\cap C)\cup(B\cap C)$，这里 A, B, C 是全集 E 的子集，对于 $\psi_A(x)$, $\psi_B(x)$ 和 $\psi_C(x)$ 的值的所有可能组合，试求出 $\psi_S(x)$ 的值，并构成集的成员表。

(4) 设 $\underset{\sim}{A}$, $\underset{\sim}{B}$ 是 U 上的两个模糊子集，它们的并集 $\underset{\sim}{A}\cup\underset{\sim}{B}$ 和交集 $\underset{\sim}{A}\cap\underset{\sim}{B}$ 都仍然是模糊子集，它们的隶属函数分别定义为：

$$\underset{\sim}{C}=\underset{\sim}{A}\cup\underset{\sim}{B}\Leftrightarrow\mu_{\underset{\sim}{C}}=\max(\mu_{\underset{\sim}{A}},\ \mu_{\underset{\sim}{B}})$$

$$\underset{\sim}{C}=\underset{\sim}{A}\cap\underset{\sim}{B}\Leftrightarrow\mu_{\underset{\sim}{C}}=\min(\mu_{\underset{\sim}{A}},\ \mu_{\underset{\sim}{B}})$$

证明　模糊集的 ∪ 和 ∩ 运算满足幂等律、交换律、结合律、吸收律、分配律、德·摩根律等。

4-4 基数的概念

为了比较两个集合的"大小",确定有限集和无限集的概念,这里首先需要引进自然数集合。

定义 4-4.1 给定集合 A 的后继集定义为集合:

$$A^+ = A \cup \{A\}。$$

若 A 为空集 $\emptyset$, 则后继集为 $\emptyset^+$, $(\emptyset^+)^+$, $((\emptyset^+)^+)^+$, …这些集合可写成如下形式:

$$\emptyset \cup \{\emptyset\},\ \emptyset \cup \{\emptyset\} \cup \{\emptyset \cup \{\emptyset\}\},$$

$$\emptyset \cup \{\emptyset\} \cup \{\emptyset \cup \{\emptyset\}\} \cup \{\emptyset \cup \{\emptyset\} \cup \{\emptyset \cup \{\emptyset\}\}\},\ \cdots。$$

可简化为:

$$\{\emptyset\},\ \{\emptyset, \{\emptyset\}\},\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \cdots$$

若我们命名集合 $\emptyset$ 为 0, 那么,

$$\emptyset^+ = 0^+ = \{\emptyset\} = 1$$

$$1^+ = \{\emptyset, \{\emptyset\}\} = 2$$

$$2^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = 3$$

$$\cdots$$

这样就得到了自然数集合{0, 1, 2, 3, …}, 这个集合亦能概括为如下公理形式(G. Peano 公理)。

1) $0 \in N$(其中 $0 = \emptyset$)。

2) 如果 $n \in N$, 那么 $n^+ \in N$(其中 $n^+ = n \cup \{n\}$)。

3) 如果一个子集 $S \subseteq N$ 具有性质:

a) $0 \in S$。

b) 如果 $n \in S$, 有 $n^+ \in S$, 则 $S = N$。

性质 3) 称极小性质, 它指明了自然数系统的最小性, 即自然数系统是满足公理 1) 和 2) 的最小集合。

当然, 自然数集, 亦可不从 0 开始, 这只需定义 $\emptyset$ 为 1 则自然数集就从 1 开始。

从上述定义可以看到任意一个自然数可看作是一个集合的

名。此外，从实际生活中我们知道任意自然数，例如 3 这个概念是从观察许多只含三个元素的集合的共同特点而加以抽象概括出来的，这个共同特点就是体现于这些被观察的任意一个集合的元素都可与集合 $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ 中元素存在一一对应，且其任意两个集合的元素之间也存在一一对应。由此可见，"对应"是集合之间进行比较的一个非常重要的概念。

定义 4-4.2 给定两个集合 P 与 Q，如果我们对 P 中每个不同元素，与 Q 中每个不同元素，可以分别两两成对，那么我们说 P 的元素与 Q 的元素间，存在着一一对应。

例如，$\{2, 4, 6, 8, \cdots, 2n, \cdots\}$ 与 $\{1, 3, 5, \cdots, 2n-1, \cdots\}$ 之间存在着一一对应的。

定义 4-4.3 当且仅当集合 A 的元素与集合 B 的元素之间存在着一一对应，集合 A 与集合 B 称为是等势的(或称同浓的)。记作 $A \sim B$。

例题 1 验证自然数集 N 与非负偶数集合 M 是等势的。

证明 因为 N 与 M 的元素之间可作一一对应的映射，即

$$f(n)=2n$$

例题 2 设 P 为实数集合，S 是 P 的子集，即 $S \subseteq P$，且

$$S=\{x \mid x \in P \wedge 0<x<1\},$$

证明

$$S \sim P$$

证明 令 $f: P \to S$

$$f(x)=\frac{1}{\pi} \operatorname{tg}^{-1} x+\frac{1}{2}(-\infty<x<\infty)$$

显然 f 的值域是 S，且 f 是双射函数。

定理 4-4.1 在集合族上等势关系是一个等价关系。

证明 设集合族为 S

a) 对任意 $A \in S$，必有 $A \sim A$。

b) 若 $A, B \in S$，如果 $A \sim B$，必有 $B \sim A$。

c) 若 $A, B, C \in S$，如果 $A \sim B$ 且 $B \sim C$，必有 $A \sim C$。 □

定义 4-4.4 如果有一个从集合 $\{0, 1, \cdots, n-1\}$ 到 A 的双

射函数，那么称集合 A 是有限的；如果集合 A 不是有限的，则它是无限的。

定理 4-4.2 自然数集合 N 是无限的。

证明 设 n 是 N 的任意元素，f 是任意的从 $\{0, 1, \cdots, n-1\}$ 到 N 的函数。设 $k=1+\max\{f(0), f(1), \cdots, f(n-1)\}$，那么 $k\in N$，但对每一个 $x\in\{0, 1, \cdots, n-1\}$，有 $f(x)\neq k$。因此 f 不能是入射函数，即 f 也不是双射函数。因为 n 和 f 都是任意的，故 N 是无限的。 □

对于有限集的大小概念很易理解，对于无限集的度量要考虑到集合的等势关系。

设有集合 A，一切与该集合等势的集合，其元素之间可以一一对应，若以此作为度量标准，我们可有如下定义。

定义 4-4.5 所有与集合 A 等势的集合所组成的集合，叫做集合 A 的基数，记为 $K[A]$（或 $\overline{\overline{A}}$）。

从基数的定义可以看到，有限集合的基数就是其元素的个数。

例如，$A=\{a, b, c\}$，$B=\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$，$C=$｛桌、灯泡，教室｝，…，因为 $A\sim B\sim C$，即 $K[A]=K[B]=K[C]$。

$$K[A]=\{A, B, C, \cdots\}$$

可以看到，如果两个集合能够建立双射函数，则两集合元素间必一一对应，从基数的定义可以知道，该两集合应具有相同的基数。

例题 3 证明区间 $[0, 1]$ 与 $(0, 1)$ 基数相同。

证明 设集合 $A=\left\{0, 1, \frac{1}{2}, \cdots, \frac{1}{n}, \cdots\right\}$，$A\subseteq[0, 1]$

定义 $f: [0, 1]\to(0, 1)$ 使得：

$$\begin{cases} f(0)=\frac{1}{2} \\ f\left(\frac{1}{n}\right)=\frac{1}{n+2} & \text{对 } n\geqslant 1 \\ f(x)=x & \text{对 } x\in[0, 1]-A \end{cases}$$

则 f 是双射函数，如图 4-4.1 所示。

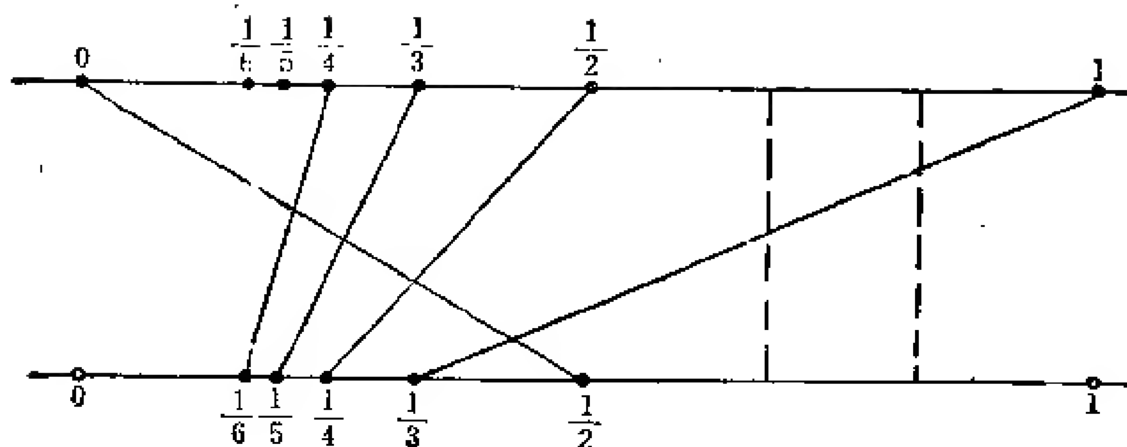


图 4-4.1

4-4 习题

(1) 对下述每组集合 A 和 B，构造一个从 A 到 B 的双射函数，说明 A 和 B 具有相同的势。

a) $A=(0, 1)$, $B=(0, 2)$

b) $A=N$, $B=N\times N$

c) $A=I\times I$, $B=N$

d) $A=R$, $B=(0, \infty)$

e) $A=[0, 1)$, $B=\left(\frac{1}{4}, \frac{1}{2}\right]$

(2) 证明 $(0, 1)$ 与 $[0, 1)$ 等势，$[0, 1)$ 与 $[0, 1]$ 等势。

(3) 若 $X_1\sim X_2$，和 $Y_1\sim Y_2$，且 $X_1\cap Y_1=X_2\cap Y_2=\emptyset$，证明 $X_1\cup Y_1\sim X_2\cup Y_2$

(4) 若 $A\sim C$ 和 $B\sim D$，证明 $A\times B\sim C\times D$。

4-5 可数集与不可数集

在上节中，我们提到自然数集 N 是无限的。但是并非所有无限集都可与自然数集建立一一对应。

定义 4-5.1 与自然数集合等势的任意集合称为可数的，可数集合的基数用 $\aleph_0$ 表示。

例如，$A=\{1, 4, 9, 16, \cdots, n^2, \cdots\}$

$B=\{1, 8, 27, 64, \cdots, n^3, \cdots\}$

$$C=\{3,\ 12,\ 27,\ \cdots,\ 3n^2,\ \cdots\}$$

$$D=\left\{1,\ \frac{1}{2},\ \frac{1}{3},\ \cdots,\ \frac{1}{n},\ \cdots\right\}$$

均为可数集。

我们把有限集和可数集统称为至多可数集。

定理 4-5.1 A 为可数集的充分必要条件是可以排列成

$$A=\{a_1,\ a_2,\ \cdots,\ a_n,\ \cdots\}$$

的形式。

证明 若 A 可排成上述形式，那么将 A 的元素 a_n 与足标 n 对应，就得到 A 与 N 之间的一一对应，故 A 是可数集。

反之，若 A 为可数集，那么在 A 与 N 之间存在一种一一对应关系 f，由 f 得到 n 的对应元素 a_n，即 A 可写为 $\{a_1, a_2, \cdots, a_n, \cdots\}$ 的形式。 □

定理 4-5.2 任一无限集，必含有可数子集。

证明 设 A 为无限集合，从 A 中取出一个元素 a_1，因为 A 是无限的，它不因取出 a_1 而耗尽，所以从 $A-\{a_1\}$ 中可取元素 a_2，则 $A-\{a_1,\ a_2\}$ 也是非空集，所以又可取一元素 a_3，如此继续下去，就得到 A 的可数子集。 □

定理 4-5.3 任一无限集合必与其某一真子集等势。

证明 设无限集合 M，按定理 4-5.2，必含有可数子集 $A=\{a_1,\ a_2,\ \cdots,\ a_n,\ \cdots\}$，设 $M-A=B$，我们定义集合 M 到其自身的映象，f：$M\to M-\{a_1\}$，使得 $f(a_n)=a_{n+1}(n=1,\ 2,\ \cdots)$ 且对于任何 $b\in B$，有 $f(b)=b$。这个 f 是双射的。 □

这个定理亦可用图4-5.1所示。

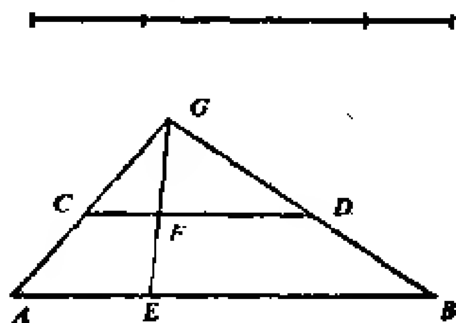


图 4-5.1

设线段 AB，其上有线段 CD，则线段 AB 与 CD 上所有的点，可作成一一对应。其作法是：把 CD 移出与 AB 平行，联 AC、BD 延长交于 G，则 AB 上任意点 E 与 G 的联线 EG 必与 CD 交于 F。

反之，CD 上任意点 F，与 G 的联线 FG 延长必交 AB 于 E，上述 E，F 的对应作法，即说明 $AB\sim CD$。 □

定理 4-5.4 可数集的任何无限子集是可数的。

证明 设 A 为可数集合，$B\subseteq A$ 为一无限子集，如将 A 的元素排成 a_1, a_2, $\cdots$, a_n, $\cdots$，从 a_1 开始，向后检查，不断地删去不在 B 中的元素，则得到新的一列 a_{i_1}, a_{i_2}, $\cdots$, a_{i_n}, $\cdots$，它与自然数一一对应，所以 B 是可数的。 □

定理 4-5.5 可数个两两不相交的可数集合的并集，仍然是一可数集。

证明 设可数个可数集分别表示为：

$$S_1=\{a_{11},\ a_{12},\ a_{13},\ \cdots,\ a_{1n},\ \cdots\}$$
$$S_2=\{a_{21},\ a_{22},\ a_{23},\ \cdots,\ a_{2n},\ \cdots\}$$
$$S_3=\{a_{31},\ a_{32},\ a_{33},\ \cdots,\ a_{3n},\ \cdots\}$$
$$\vdots$$

令 $S=S_1\cup S_2\cup S_3\cup\cdots$，即 $S=\bigcup\limits_{k=1}^{\infty}S_k$，对 S 的元素作如下排列：

$$\begin{array}{ccccccccc}
a_{11} & & a_{12} & & a_{13} & & a_{14} & & \cdots \\
\downarrow & \nearrow & & \nearrow & & \nearrow & & & \\
a_{21} & & a_{22} & & a_{23} & & a_{24} & & \cdots \\
& \nearrow & & \nearrow & & & & & \\
a_{31} & & a_{32} & & a_{33} & & a_{34} & & \cdots \\
& \nearrow & & & & & & & \\
a_{41} & & a_{42} & & a_{43} & & a_{44} & & \cdots \\
\vdots & & & & & & & &
\end{array}$$

在上述元素的排列中，由左上端开始，其每一斜线上的每一元素的两足码之和都相同，依次为 2, 3, 4, $\cdots$，各斜线上元素的个数依次为 1, 2, 3, 4, $\cdots$，故

$$S=\bigcup_{k=1}^{\infty}S_k$$

的元素可排列为：

$$a_{11},\ a_{21},\ a_{12},\ a_{31},\ a_{22},\ a_{13},\ \cdots$$ □

定理 4-5.6 设自然数集合 N，则 $N\times N$ 是可数集。

证明 首先我们把 $N\times N$ 的元素足码按表 4-5.1 的次序排列，并对表中每个序偶注以标号。

表 4-5.1

0	1	3	6	10	
⟨0, 0⟩	⟨0, 1⟩	⟨0, 2⟩	⟨0, 3⟩	⟨0, 4⟩	⋯
2 ↙	4 ↙	7 ↙	11 ↙		
⟨1, 0⟩	⟨1, 1⟩	⟨1, 2⟩	⟨1, 3⟩	⟨1, 4⟩	⋯
5 ↙	8 ↙	12 ↙			
⟨2, 0⟩	⟨2, 1⟩	⟨2, 2⟩	⟨2, 3⟩	⟨2, 4⟩	⋯
9 ↙	13 ↙				
⟨3, 0⟩	⟨3, 1⟩	⟨3, 2⟩	⟨3, 3⟩	⟨3, 4⟩	⋯
14 ↙					
⟨4, 0⟩	⟨4, 1⟩	⟨4, 2⟩	⟨4, 3⟩	⟨4, 4⟩	⋯

我们可以作 $f: N\times N\to N$ 如下：

$$f(m, n)=\frac{1}{2}(m+n)(m+n+1)+m$$

若把 $f(m, n)$ 看作表 4-5.1 中序偶 $\langle m, n\rangle$ 的标号，则

$$f: N\times N\to N$$

是个双射函数。这是因为：

a)

$$f(0, 1)-f(0, 0)=1$$
$$f(0, 2)-f(0, 1)=2$$
$$f(0, 3)-f(0, 2)=3$$
$$\vdots \qquad \vdots$$
$$f(0, n)-f(0, n-1)=n$$

则
$$f(0, n)-f(0, 0)=\frac{n(n+1)}{2}$$

因为
$$f(0, 0)=0$$

故
$$f(0, n)=\frac{n(n+1)}{2}$$

又
$$f(1, n)-f(0, n)=n+2$$
$$f(2, n)-f(1, n)=n+3$$
$$\vdots \qquad \vdots$$
$$f(m, n)-f(m-1, n)=m+n+1$$

所以 $$f(m, n)-f(0, n)=mn+\frac{m(m+3)}{2}$$

$$f(m, n)=\frac{n(n+1)}{2}+\frac{m(m+3)}{2}+mn$$

经整理得:

$$f(m, n)=\frac{1}{2}(m+n)(m+n+1)+m \tag{A}$$

b) 若给出 $f(m, n)\in N$, 可由(A)式确定唯一序偶 $\langle m, n\rangle$。

因 $$f(m, n)=\frac{1}{2}(m+n)(m+n+1)+m$$

其中 $m, n\in N$。

令 $$u=f(m, n)$$

则 $$u\geqslant\frac{1}{2}(m+n)(m+n+1)$$

$$u<\frac{1}{2}(m+n)(m+n+1)+(m+n)+1$$

$$=\frac{1}{2}(m+n)(m+n+3)+1$$

令 $m+n=A$, 则

$$\frac{1}{2}A(A+1)\leqslant u<\frac{1}{2}A(A+3)+1$$

即 $$A^2+A-2u\leqslant 0$$

$$A^2+3A-2(u-1)>0$$

$$-1+\frac{-1+\sqrt{1+8u}}{2}<A\leqslant\frac{-1+\sqrt{1+8u}}{2}$$

因为 A 是自然数,故可取

$$A=\left[\frac{-1+\sqrt{1+8u}}{2}\right]^{[注]}$$

因此, $$\begin{cases} m=u-\dfrac{1}{2}A(A+1) \\ n=A-m \end{cases}$$

由 a), b) 可知 $N\times N$ 是可数的。 □

[注] $[x]$表示 x 的整数部分。

定理 4-5.7 有理数的全体组成的集合是可数集。

证明　由定理 4-5.6 中可知 $N\times N$ 是可数的，在 $N\times N$ 集合中删除所有 m 和 n 不是互为质数的序偶 $\langle m, n\rangle$，得集合 $S\subseteq N\times N$，$S=\{\langle m, n\rangle \mid m\in N, n\in N$ 且 m 和 n 互质$\}$。因为 S 是 $N\times N$ 的无限子集，故据定理 4-5.4 可知，S 是可数的。

令 $g: S\to Q_+$ 即 $g: \langle m, n\rangle\to m/n$(其中 m, n 互质)，因为 g 是双射，故 Q_+ 是可数集。又因为 $Q_+\sim Q^-$，故

$$Q=Q_+\cup\{0\}\cup Q^-$$

是可数集。 □

定理 4-5.8 全体实数构成的集合 R 是不可数的。

证明　因为 f: $(0, 1)\to R$ 是双射函数，令

$$S=\{x \mid x\in R\wedge(0<x<1)\}$$

若能证 S 是不可数集，则 R 也必为不可数集。

用反证法。

假设 S 是可数的，则 S 必可表示为：$S=\{S_1, S_2, \cdots\}$，其中 S_i 是 $(0, 1)$ 间的任一实数。

设 $S_i=0.y_1y_2y_3\cdots$，其中 $y_i\in\{0, 1, 2, \cdots, 9\}$ (如 0.2 和 0.123 可记为 0.1999… 和 0.12999…)，

设
$$S_1=0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots$$
$$S_2=0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots$$
$$S_3=0.a_{31}a_{32}a_{33}\cdots a_{3n}\cdots$$
$$\cdots$$

其次，我们构造一个实数 $r=0.b_1b_2b_3\cdots$ 使

$$b_j=\begin{cases}1 & a_{jj}\neq 1\\ 2 & a_{jj}=1\end{cases}\quad j=1, 2, \cdots$$

这样，r 与所有实数 $S_1, S_2, \cdots, S_n, \cdots$ 不同，因为它与 S_1 在位置 1 不同，与 S_2 在位置 2 不同，…，等等。这证明了 $r\notin S$，产生矛盾，因此 S 是不可数的，即 R 是不可数集。 □

我们把集合 $(0, 1)$ 的基数记为“$\aleph$”，因为 $(0, 1)\sim R$，故 $K[R]=\aleph$。“$\aleph$”也称作连续统的势。

4-5 习题

(1) 下列集合 A 的势是什么?

a) $A=\{\langle p, q\rangle | p、q$ 都是整数$\}$;

b) $A=\{\langle p, q\rangle | p、q$ 都是有理数$\}$;

c) A 是由所有半径为 1, 圆心在 x 轴上的圆周所组成的集合;

d) A 是由实数轴上所有两两不相交的有限开区间组成的集合。

(2) 如果 A 是不可数无穷集, B 是 A 的可数子集, 则$(A-B)\sim A$。

(3) 如果 A 是任意无限集, M 是一个可数集, 则$(A\cup M)\sim A$。

(4) 如果两集合 A_1 和 A_2 都是可数的, 证明 $A_1\times A_2$ 也是可数的。

(5) 有限集和可数集 B 的笛卡尔积集 $A\times B$ 是可数集。

(6) 若 S 为无理数集, 证明 $K[S]=\aleph$。

(7) 令 $K[A]=\aleph$, $K[B]=\aleph$, $K[D]=\aleph_0$, 这里A、B、D 为互不相交集合, 证明以下各式:

(a) $K[A\cup B]=\aleph$　　　　(b) $L[A\cup D]=\aleph$

4-6 基数的比较

在上一节我们论述了可数集和一些不可数集的基数概念。为了证明两个集合的基数相等, 我们必须构造两个集合之间的双射函数, 这常常是非常困难的工作。下面将介绍证明基数相等的一个较为简单的方法, 为此先说明基数是如何比较大小的。

定义 4-6.1 若从集合 A 到集合 B 存在一个入射, 则称 A 的基数不大于 B 的基数, 记作 $K[A]\leqslant K[B]$。若从 A 到 B 存在一个入射, 但不存在双射, 则称 A 的基数小于 B 的基数, 记作 $K[A]<K[B]$。

下面二个定理限于篇幅, 不予证明, 但可以举例说明其广泛的应用。

定理 4-6.1 (Zermelo 定理) 令 A 和 B 是任意集合, 则以下三条中恰有一条成立。

a) $K[A]<K[B]$

b) $K[B]<K[A]$

c) $K[A]=K[B]$ □

定理 4-6.2(Cantor-Schroder-Bernstein 定理) 设 A 和 B 是集合，如果 $K[A]\leqslant K[B]$, $K[B]\leqslant K[A]$，则

$$K[A]=K[B]$$ □

这个定理对证明集合有相同的基数提供了有效方法，如果我们能够构造一入射函数 f: $A\to B$，即说明有 $K[A]\leqslant K[B]$，另外，如能够构造入射函数 g: $B\to A$，即有 $K[B]\leqslant K[A]$，因此根据本定理就得到 $K[A]=K[B]$。

例题 1 证明[0, 1]与(0, 1)有相同的基数。

证明 作入射函数：

$$f:\ (0,1)\to[0,1],\ f(x)=x$$

$$g:\ [0,1]\to(0,1),\ g(x)=\frac{x}{2}+\frac{1}{4}$$

例题 2 设 $A=N$, $B=(0,1)$, $K[A]=\aleph_0$, $K[B]=\aleph$，求证

$$K[A\times B]=\aleph$$

证明 定义一个从 $A\times B$ 到正实数的函数 f。

$$f:\ A\times B\to\{x\mid x\in R_+\}$$

$$f(n,x)=n+x$$

因为 f 是入射函数，且 $K[R_+]=\aleph$，所以 $K[A\times B]\leqslant\aleph$。此外，作映射 g: $(0,1)\to A\times B$

$$g(x)=\langle 0,x\rangle$$

因为 g 是入射的，故 $\aleph\leqslant K[A\times B]$。因此

$$K[A\times B]=\aleph$$

定理 4-6.3 设 A 是有限集合，则 $K[A]<\aleph_0<\aleph$。

证明 设 $K[A]=n$，则 $A\sim\{0,1,2,\cdots,n-1\}$。定义函数 f: $\{0,1,2,\cdots,n-1\}\to N$, $f(x)=x$; f 是入射函数，故

$$K[A]\leqslant K[N]$$

在定理 4-4.2 中已证得 N 到 A 之间不存在双射函数，所以

$$K[A]\neq K[N]$$

故 $K[A]<K[N]$，即 $K[A]<\aleph_0$。

又作映射 g: $N \to [0, 1]$，$g(n) = \frac{1}{n+1}$，g 是入射函数，故 $\aleph_0 \leqslant \aleph$。

因为 N 与 $[0, 1]$ 间不能一一对应，故 $\aleph_0 \neq \aleph$，因此 $\aleph_0 < \aleph$。

□

定理 4-6.4 如果 A 是无限集，那么 $\aleph_0 \leqslant K[A]$。

证明 因为 A 是无限集合，故 A 必包含一个可数无限子集 A'，作函数 f: $A' \to A$，使得 $f(x) = x$，对 $x \in A'$，f 是入射函数，故 $K[A'] \leqslant K[A]$。

但 $K[A'] = \aleph_0$，因此 $\aleph_0 \leqslant K[A]$。 □

尽管我们证明了 $\aleph_0 < \aleph$，以及 $\aleph_0 \leqslant K[A]$。但是直到目前为止还没有人能够证明是否有一无限集，其基数严格介于 $\aleph_0$ 与 $\aleph$ 之间。

假定 $\aleph$ 是大于 $\aleph_0$ 的最小基数，即不存在任何基数 $K[S]$，使 $\aleph_0 < K[S] < \aleph$ 成立，这就是著名的连续统假设。

最后我们指出，没有最大的基数和没有最大的集合。

定理 4-6.5 (Cantor 定理) 设 M 是一个集合，$T = \mathscr{P}(M)$

则
$$K[M] < K[T]$$

证明 a) 首先证明 $K[M] \leqslant K[T]$。为此作函数 f: $M \to \mathscr{P}(M)$，使得 $f(a) = \{a\}$，则 f 是入射函数，故 $K[M] \leqslant K[T]$。

b) 其次我们证明 $K[M] \neq K[T]$。

反之，若 $K[M] = K[T]$，则必有函数 φ: $M \to T$ 是双射函数。对于任意 $m \in M$，必有 T 中唯一的 $\varphi(m)$ 与之对应，即 $m \to \varphi(m)$。

若 $m \in \varphi(m)$ 称 m 为 M 的内部元素，若 $m \notin \varphi(m)$ 称 m 为 M 的外部元素。

设 $S = \{x \mid x \in M, x \notin \varphi(x)\}$，即 S 为 M 的外部元素集合，则有 $S \subseteq M$，故 $S \in T$。

因为 φ 是双射函数，故必有一个元素 $b \in M$，使

$$\varphi(b) = S$$

若 $b\in S$，因为 $\varphi(b)=S$，此时 b 为 M 的内部元素，得出矛盾。

若 $b\notin S$，因为 $\varphi(b)=S$，此时 b 为 M 的外部元素，也得出矛盾。

故 $K[M]\neq K[T]$，由 a)，b) 得到 $K[M]<K[T]$。 □

4-6 习题

(1) 用定理 4-6.2 证明[0, 1]、(0, 1]、[0, 1)、(0, 1)是等势的。

(2) 证明若从 A 到 B 存在一个满射，则 $K[B]\leqslant K[A]$。

(3) 设 N 为自然数集，证明 $K[\mathscr{P}(N)]=\aleph$。

(4) 证明 $K[N^N]=\aleph$。

(5) 设 A、B、D 都是集合且 $A\cap B=\phi$，$K[A]=a$，$K[B]=b$，$K[D]=d$，若定义 $a+b=K[A\cup B]$，$a\cdot b=K[A\times B]$，

求证：

a) $\aleph+\aleph_0=\aleph$

b) 如果 $a\leqslant b$，则 $a+d\leqslant b+d$

c) 如果 $a\leqslant b$，则 $ad\leqslant bd$

第三篇 代数系统

人们研究和考察现实世界中的各种现象或过程，往往要借助某些数学工具。譬如，在微积分学中，可以用导数来描述质点运动的速度，可以用定积分来计算面积、体积等；在代数学中，可以用正整数集合上的加法运算来描述工厂产品的累计数，可以用集合之间的“并”、“交”运算来描述单位与单位之间的关系等。针对某个具体问题选用适宜的数学结构去进行较为确切的描述，这就是所谓的“数学模型”。可见，数学结构在数学模型中占有极为重要的位置。我们这里所要研究的是一类特殊的数学结构——由集合上定义若干个运算而组成的系统。我们通常称它为代数系统。它在计算机科学中有着广泛的应用。

第五章　代数结构

本章将从一般代数系统的引入出发，研究一些特殊的代数系统，而这些代数系统中的运算具有某些性质，从而确定了这些代数系统的数学结构。

5-1　代数系统的引入

在介绍代数系统之前，先引进在一个集合 A 上的运算概念。例如，将实数集合 R 上的每一个数 $a\neq 0$ 映射成它的倒数 $\frac{1}{a}$，或者将 R 上的每一个数 y 映射成 $\lceil y\rceil$，就可以将这些映射称为在集合 R 上的一元运算；而在集合 R 上，对任意两个数所进行的普通加法和乘法，都是集合 R 上的二元运算，也可以看作是将 R 上的每二个数映射成 R 中的一个数；至于对集合 R 上的任意三个数 x, y, z, ALGOL 算法语言中的条件算术表达式 if $x=0$ then y else z，就是集合 R 上的三元运算。上述一些例子，有一个共同的特征，那就是其运算结果都是在原来的集合 R 中，我们称那些具有这种特征的运算是封闭的，简称闭运算。相反地，没有这种特征的运算就是不封闭的。

很容易举出不封闭运算的例子：一架自动售货机，能接受一角硬币和二角伍分硬币，而所对应的商品是桔子水(瓶)、可口可乐(瓶)和冰淇淋(杯)。当人们投入上述硬币的任何两枚时，自动售货机将按表 5-1.1 所示的供应相应的商品。

表格左上角的记号 * 可以理解为一个二元运算的运算符。这个例子中的二元运算 * 就是集合{一角硬币，二角伍分硬币}上的不封闭运算。

表 5-1.1

*	一角硬币	二角伍分硬币
一角硬币	桔子水	可口可乐
二角伍分硬币	可口可乐	冰淇淋

定义 5-1.1 对于集合 A，一个从 A^n 到 B 的映射，称为集合 A 上的一个 n 元运算。如果 $B \subseteq A$，则称该 n 元运算是封闭的。

定义 5-1.2 一个非空集合 A 连同若干个定义在该集合上的运算 $f_1, f_2, \cdots, f_k$ 所组成的系统就称为一个代数系统，记作 $\langle A, f_1, f_2, \cdots, f_k \rangle$。

如正整数集合 I_+ 以及在该集合上的普通加法运算"+"组成一个代数系统 $\langle I_+, + \rangle$。又如，一个有限集 S，由 S 的幂集 $\mathscr{P}(S)$ 以及在该幂集上的集合运算"∪"、"∩"、"~"组成一个代数系统 $\langle \mathscr{P}(S), \cup, \cap, \sim \rangle$。虽然，有些代数系统具有不同的形式，但是，它们之间可能有一些共同的运算规律。

例如，考察代数系统 $\langle I, + \rangle$，这里 I 是整数集合，+是普通的加法运算。很明显，在这个代数系统中，关于加法运算，具有以下三个运算规律，即对于任意的 $x, y, z \in I$，有

(1) $x+y \in I$ (封闭性)

(2) $x+y=y+x$ (交换律)

(3) $(x+y)+z=x+(y+z)$ (结合律)

容易找到与 $\langle I, + \rangle$ 具有相同运算规律的一些代数系统，如表 5-1.2 所示。

表 5-1.2

	$\langle I, \cdot \rangle$	$\langle R, + \rangle$	$\langle \mathscr{P}(S), \cup \rangle$	$\langle \mathscr{P}(S), \cap \rangle$
集合	I 为整数集合	R 为实数集合	$\mathscr{P}(S)$ 是 S 的幂集	$\mathscr{P}(S)$ 是 S 的幂集
运算	· 为普通乘法	+ 为普通加法	∪ 为集合的"并"	∩ 为集合的"交"
封闭性	$x \cdot y \in I$	$x+y \in R$	$A \cup B \in \mathscr{P}(S)$	$A \cap B \in \mathscr{P}(S)$
交换律	$x \cdot y = y \cdot x$	$x+y=y+x$	$A \cup B = B \cup A$	$A \cap B = B \cap A$
结合律	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	$(x+y)+z = x+(y+z)$	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$

5-1 习题

(1) 设集合 $A=\{1, 2, 3, \cdots, 10\}$，问下面定义的二元运算 * 关于集合 A 是否封闭？

a) $x*y=\max(x, y)$

b) $x*y=\min(x, y)$

c) $x*y=\mathrm{GCD}(x, y)$

d) $x*y=\mathrm{LCM}(x, y)$

e) $x*y=$质数 p 的个数，使得 $x\leqslant p\leqslant y$

(2) 在下表所列出的集合和运算中，请根据运算的是否封闭，在相应的位置上填写"是"或"否"(其中，N 是自然数集合)。

是否封闭 / 集合	运			算			
	$+$	$-$	$\cdot$	$\lvert x-y\rvert$	max	min	$\lvert x\rvert$
I							
N							
$\{x\mid 0\leqslant x\leqslant 10\}$							
$\{x\mid -10\leqslant x\leqslant 10\}$							
$\{2x\mid x\in I\}$							

(3) 试列举你所熟悉的一些代数系统。

5-2 运算及其性质

在前面考察几个具体的代数系统时，已经涉及到我们所熟知的运算的某些性质。下面，着重讨论一般二元运算的一些性质。

定义 5-2.1 设 * 是定义在集合 A 上的二元运算，如果对于任意的 $x, y\in A$，都有 $x*y\in A$，则称二元运算 * 在 A 上是封闭的。

例题 1 设 $A=\{x\mid x=2^n, n\in N\}$，问乘法运算是否封闭？对加法运算呢？

解 对于任意的 $2^r, 2^s\in A$，$r, s\in N$，因为 $2^r\cdot 2^s=2^{r+s}\in A$ 所以乘法运算是封闭的。而对于加法运算是不封闭的，因为至少有 $2+2^2=6\notin A$。

定义 5-2.2 设 $*$ 是定义在集合 A 上的二元运算，如果对于任意的 x, $y\in A$，都有 $x*y=y*x$，则称该二元运算 $*$ 是可交换的。

例题 2 设 Q 是有理数集合，$\triangle$ 是 Q 上的二元运算，对任意的 a, $b\in R$, $a\triangle b=a+b-a\cdot b$，问运算 $\triangle$ 是否可交换。

解 因为

$$a\triangle b=a+b-a\cdot b=b+a-b\cdot a=b\triangle a$$

所以运算 $\triangle$ 是可交换的。

定义 5-2.3 设 $*$ 是定义在集合 A 上的二元运算，如果对于任意的 x, y, $z\in A$ 都有 $(x*y)*z=x*(y*z)$，则称该二元运算 $*$ 是可结合的。

例题 3 设 A 是一个非空集合，★是 A 上的二元运算，对于任意 a, $b\in A$，有 $a★b=b$，证明★是可结合运算。

证明 因为对于任意的 a, b, $c\in A$

$$(a★b)★c=b★c=c$$

而

$$a★(b★c)=a★c=c$$

所以

$$(a★b)★c=a★(b★c)$$

定义 5-2.4 设 $*$, $\triangle$ 是定义在集合 A 上的两个二元运算，如果对于任意的 x, y, $z\in A$，都有

$$x*(y\triangle z)=(x*y)\triangle(x*z)$$

$$(y\triangle z)*x=(y*x)\triangle(z*x)$$

则称运算 $*$ 对于运算 $\triangle$ 是可分配的。

例题 4 设集合 $A=\{\alpha, \beta\}$，在 A 上定义两个二元运算 $*$ 和 $\triangle$ 如表 5-2.1 所示。运算 $\triangle$ 对于运算 $*$ 可分配吗？运算 $*$ 对于运算 $\triangle$ 呢？

表 5-2.1

$*$	α	β
α	α	β
β	β	α

$\triangle$	α	β
α	α	α
β	α	β

解 容易验证运算 $\triangle$ 对于运算 $*$ 是可分配的。但是运算 $*$ 对于运算 $\triangle$ 是不可分配的，因为

$$\beta*(\alpha\triangle\beta)=\beta*\alpha=\beta$$

而 $$(\beta*\alpha)\triangle(\beta*\beta)=\beta\triangle\alpha=\alpha。$$

定义 5-2.5 设 $*$, $\triangle$ 是定义在集合 A 上的两个可交换二元运算,如果对于任意的 $x, y\in A$, 都有

$$x*(x\triangle y)=x$$

$$x\triangle(x*y)=x$$

则称运算 $*$ 和运算 $\triangle$ 满足吸收律。

例题 5 设集合 N 为自然数全体, 在 N 上定义两个二元运算 $*$ 和 ★, 对于任意 $x, y\in N$, 有

$$x*y=\max(x, y)$$

$$x★y=\min(x, y)$$

验证运算 $*$ 和 ★ 的吸收律。

解 对于任意 $a, b\in N$

$$a*(a★b)=\max(a, \min(a, b))=a$$

$$a★(a*b)=\min(a, \max(a, b))=a$$

因此, $*$ 和 ★ 满足吸收律。

定义 5-2.6 设 $*$ 是定义在集合 A 上的一个二元运算, 如果对于任意的 $x\in A$, 都有 $x*x=x$,则称运算 $*$ 是等幂的。

例题 6 设 $\mathscr{P}(S)$是集合 S 的幂集, 在 $\mathscr{P}(S)$上定义的两个二元运算,集合的"并"运算 $\cup$ 和集合的"交"运算 $\cap$,验证$\cap$, $\cup$ 是等幂的。

解 对于任意的 $A\in\mathscr{P}(S)$,有 $A\cup A=A$ 和 $A\cap A=A$,因此运算 $\cup$ 和 $\cap$ 都满足等幂律。

定义 5-2.7 设 $*$ 是定义在集合 A 上的一个二元运算, 如果有一个元素 $e_l\in A$, 对于任意的元素 $x\in A$ 都有 $e_l*x=x$, 则称 e_l 为 A 中关于运算 $*$ 的左幺元; 如果有一个元素 $e_r\in A$, 对于任意的元素 $x\in A$ 都有 $x*e_r=x$, 则称 e_r 为 A 中关于运算 $*$ 的右幺元; 如果 A 中的一个元素 e,它既是左幺元又是右幺元, 则称 e 为 A 中关于运算 $*$ 的幺元。显然,对于任一 $x\in A$, 有 $e*x=x*e=x$。

例题 7 设集合 $S=\{\alpha, \beta, \gamma, \delta\}$, 在 S 上定义的两个二元运算 $*$ 和 ★ 如表 5-2.2 所示。试指出左幺元或右幺元。

表 5-2.2

(a)

*	α	β	γ	δ
α	δ	α	β	γ
β	α	β	γ	δ
γ	α	β	γ	γ
δ	α	β	γ	δ

(b)

★	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

解　由表5-2.2可知β、δ都是S中关于运算$*$的左幺元，而α是S中关于运算★的右幺元。

定理5-2.1　设$*$是定义在集合A上的一个二元运算，且在A中有关于运算$*$的左幺元e_l和右幺元e_r，则$e_l=e_r=e$，且A中的幺元是唯一的。

证明　因为e_l和e_r分别是A中关于运算$*$的左幺元和右幺元，所以

$$e_l=e_l*e_r=e_r=e$$

设另有一幺元$e_1\in A$，则

$$e_1=e_1*e=e。$$ □

定义5-2.8　设$*$是定义在集合A上的一个二元运算，如果有一个元素$\theta_l\in S$，对于任意的元素$x\in A$都有$\theta_l*x=\theta_l$，则称θ_l为A中关于运算$*$的左零元；如果有一个元素$\theta_r\in A$，对于任意的元素$x\in A$都有$x*\theta_r=\theta_r$，则称θ_r为A中关于运算$*$的右零元；如果A中的一个元素θ，它既是左零元又是右零元，则称θ为A中关于运算$*$的零元。显然，对于任一$x\in A$，有

$$\theta*x=x*\theta=\theta$$

例题8　设集合$S=\{$浅色，深色$\}$，定义在S上的一个二元运算$*$如表5-2.3所示。

表 5-2.3

*	浅色	深色
浅　色	浅色	深色
深　色	深色	深色

试指出零元和幺元。

解　深色是 S 中关于运算 $*$ 的零元，浅色是 S 中关于运算 $*$ 的幺元。

定理 5-2.2　设 $*$ 是定义在集合 A 上的一个二元运算，且在 A 中有关于运算 $*$ 的左零元 θ_l 和右零元 θ_r，那么，$\theta_l=\theta_r=\theta$，且 A 中的零元是唯一的。

这个定理的证明与定理 5-2.1 相仿。　□

定理 5-2.3　设 $\langle A, *\rangle$ 是一个代数系统，且集合 A 中元素的个数大于 1。如果该代数系统中存在幺元 e 和零元 θ，则 $\theta\neq e$。

证明　用反证法。设 $\theta=e$，那么对于任意的 $x\in A$，必有

$$x=e*x=\theta*x=\theta=e$$

于是，A 中的所有元素都是相同的，这与 A 中含有多个元素相矛盾。　□

定义 5-2.9　设代数系统 $\langle A, *\rangle$，这里 $*$ 是定义在 A 上的一个二元运算，且 e 是 A 中关于运算 $*$ 的幺元。如果对于 A 中的一个元素 a 存在着 A 中的某个元素 b，使得 $b*a=e$，那么称 b 为 a 的左逆元；如果 $a*b=e$ 成立，那么称 b 为 a 的右逆元；如果一个元素 b，它既是 a 的左逆元又是 a 的右逆元，那么就称 b 是 a 的一个逆元。

很明显，如果 b 是 a 的逆元，那么 a 也是 b 的逆元，简称为 a 与 b 互为逆元。今后，一个元素 x 的逆元记为 x^{-1}。

一般地说，一个元素的左逆元不一定等于该元素的右逆元。而且，一个元素可以有左逆元而没有右逆元，甚至一个元素的左(右)逆元还可以不是唯一的。

例题 9　设集合 $S=\{\alpha, \beta, \gamma, \delta, \zeta\}$，定义在 S 上的一个二元运算 $*$ 如表 5-2.4 所示。

试指出代数系统 $\langle S, *\rangle$ 中各个元素的左、右逆元情况。

解　α 是幺元；β 的左逆元和右逆元都是 γ；即 β 和 γ 互为逆元；δ 的左逆元是 γ 而右逆元是 β；β 有两个左逆元 γ 和 δ；ζ 的右逆元是 γ，但 ζ 没有左逆元。

表 5-2.4

*	α	β	γ	δ	ζ
α	α	β	γ	δ	ζ
β	β	δ	α	γ	δ
γ	γ	α	β	α	β
δ	δ	α	γ	δ	γ
ζ	ζ	δ	α	γ	ζ

定理5-2.4 设代数系统$\langle A, *\rangle$，这里$*$是定义在A上的一个二元运算，A中存在幺元e，且每一个元素都有左逆元。如果$*$是可结合的运算，那么，这个代数系统中任何一个元素的左逆元必定也是该元素的右逆元，且每个元素的逆元是唯一的。

证明 设$a, b, c\in A$，且b是a的左逆元，c是b的左逆元。因为

$$(b*a)*b=e*b=b$$

所以

$$\begin{aligned}e=c*b&=c*((b*a)*b)\\&=(c*(b*a))*b\\&=((c*b)*a)*b\\&=(e*a)*b\\&=a*b\end{aligned}$$

因此，b也是a的右逆元。

设元素a有两个逆元b和c，那么

$$\begin{aligned}b=b*e=b*(a*c)&\\=(b*a)*c&\\=e*c&\\=c&\end{aligned}$$

因此，a的逆元是唯一的。 □

例题 10 试构造一个代数系统，使得其中只有一个元素具有逆元。

解：设$m, n\in I$，$T=\{x|x\in I, m\leqslant x\leqslant n\}$，那么，代数系统$\langle T, \max\rangle$中有一个幺元是$m$，且只有$m$有逆元，因为$m=\max(m, m)$。

例题 11 对于代数系统 $\langle R, \cdot \rangle$，这里 R 是实数的全体，$\cdot$ 是普通的乘法运算，是否每个元素都有逆元。

解 该代数系统中的幺元是 1，除了零元素 0 外，所有的元素都有逆元。

例题 12 对于代数系统 $\langle N_k, +_k \rangle$，这里 $N_k=\{0, 1, 2, \cdots, k-1\}$，$+_k$ 是定义在 N_k 上的模 k 加法运算，定义如下：

对于任意 $x, y \in N_k$

$$x+_k y=\begin{cases} x+y & \text{若} \quad x+y<k \\ x+y-k & \text{若} \quad x+y \geqslant k \end{cases}$$

试问是否每个元素都有逆元。

解 可以验证，$+_k$ 是一个可结合的二元运算，N_k 中关于运算 $+_k$ 的幺元是 0，N_k 中的每一个元素都有唯一的逆元，即 0 的逆元是 0，每个非零元素 x 的逆元是 $k-x$。

可以指出：$\langle A, * \rangle$ 是一个代数系统，$*$ 是 A 上的一个二元运算，那么该运算的有些性质可以从运算表中直接看出。那就是：

1. 运算 $*$ 具有封闭性，当且仅当运算表中的每个元素都属于 A。

2. 运算 $*$ 具有可交换性，当且仅当运算表关于主对角线是对称的。

3. 运算 $*$ 具有等幂性，当且仅当运算表的主对角线上的每一元素与它所在行(列)的表头元素相同。

4. A 关于 $*$ 有零元，当且仅当该元素所对应的行和列中的元素都与该元素相同。

5. A 中关于 $*$ 有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。

6. 设 A 中有幺元，a 和 b 互逆，当且仅当位于 a 所在行，b 所在列的元素以及 b 所在行，a 所在列的元素都是幺元。

5-2 习题

(1) 对于实数集合 R，下表所列的二元运算是否具有左边一列中的那些性质，请在相应的位置上填写“是”或“否”。

	$+$	$-$	$\cdot$	max	min	$\|x-y\|$
可结合性						
可交换性						
存在幺元						
存在零元						

(2) 设代数系统 $\langle A, *\rangle$，其中 $A=\{a, b, c\}$，$*$ 是 A 上的一个二元运算。对于由以下几个表所确定的运算，试分别讨论它们的交换性、等幂性以及在 A 中关于 $*$ 是否有幺元。如果有幺元，那么 A 中的每个元素是否有逆元。

a)

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

b)

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

c)

$*$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

d)

$*$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	b

(3) 证明定理 5-2.2。

(4) 举日常生活的例子，分别说明幺元，零元和逆元。

(5) 定义 I_+ 上的两个二元运算为：

$$a * b = a^b$$

$$a \triangle b = a \cdot b \qquad a, b \in I_+$$

试证明 $*$ 对 $\triangle$ 是不可分配的。

5-3 半　　群

半群是一种特殊的代数系统，它在形式语言、自动机等领域中，都有具体的应用。

定义 5-3.1 一个代数系统 $\langle S, *\rangle$，其中 S 是非空集合，$*$ 是 S 上的一个二元运算，如果运算 $*$ 是封闭的，则称代数系统 $\langle S, *\rangle$ 为广群。

定义 5-3.2 一个代数系统 $\langle S, *\rangle$，其中 S 是非空集合，$*$ 是 S 上的一个二元运算。如果：

(1) 运算 $*$ 是封闭的。

(2) 运算 $*$ 是可结合的，即对任意的 $x, y, z\in S$，满足

$$(x*y)*z=x*(y*z)$$

则称代数系统 $\langle S, *\rangle$ 为半群。

例题 1 设集合 $S_k=\{x|x\in I\wedge x\geqslant k\}$，$k\geqslant 0$，那么 $\langle S_k, +\rangle$ 是一个半群，其中+是普通的加法运算。

解 因为运算+在 S_k 上是封闭的，而且普通加法运算是可结合的。所以，$\langle S_k, +\rangle$ 是一个半群。

在例题 1 中，$k\geqslant 0$ 这个条件是重要的，否则，如果 $k<0$，则运算 $+$ 在 S_k 上将是不封闭的。

例题 2 设 $S=\{a, b, c\}$，在 S 上的一个二元运算 $\triangle$ 定义如表 5-3.1 所示。

表 5-3.1

$\triangle$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

验证 $\langle S, \triangle\rangle$ 是一个半群。

解 从表 5-3.1 中可知运算 $\triangle$ 是封闭的，同时 a，b 和 c 都是左幺元。所以，对于任意的 $x, y, z\in S$，都有

$$x\triangle(y\triangle z)=x\triangle z=z=y\triangle z=(x\triangle y)\triangle z$$

因此，$\langle S, \triangle\rangle$ 是半群。

明显地，代数系统 $\langle I_+, -\rangle$ 和 $\langle R, /\rangle$ 都不是半群，这里，$-$ 和 $/$ 分别是普通的减法和除法。

定理 5-3.1 设 $\langle S, *\rangle$ 是一个半群，$B\subseteq S$ 且 $*$ 在 B 上是封闭的，那么 $\langle B, *\rangle$ 也是一个半群。通常称 $\langle B, *\rangle$ 是半群 $\langle S, *\rangle$ 的子半群。

证明 因为 $*$ 在 S 上是可结合的，而 $B\subseteq S$ 且 $*$ 在 B 上封闭，所以 $*$ 在 B 上也是可结合的，因此，$\langle B, *\rangle$ 是一个半群。

□

例题 3 设 · 表示普通的乘法运算，那么 $\langle[0, 1], \cdot\rangle$、$\langle[0, 1), \cdot\rangle$ 和 $\langle I, \cdot\rangle$ 都是 $\langle R, \cdot\rangle$ 的子半群。

解 首先，运算·在 R 上是封闭的，且是可结合的，所以 $\langle R, \cdot\rangle$ 是一个半群。其次，运算·在 $[0, 1]$、$[0, 1)$ 和 I 上都是封闭的，且 $[0, 1]\subset R$，$[0, 1)\subset R$，$I\subset R$。因此，由定理 5-3.1 可知 $\langle[0, 1], \cdot\rangle$、$\langle[0, 1), \cdot\rangle$ 和 $\langle I, \cdot\rangle$ 都是 $\langle R, \cdot\rangle$ 的子半群。

定理 5-3.2 设 $\langle S, *\rangle$ 是一个半群，如果 S 是一个有限集，则必有 $a\in S$，使得 $a*a=a$。

证明 因为 $\langle S, *\rangle$ 是半群。对于任意的 $b\in S$，由 $*$ 的封闭性可知

$$b*b\in S, \text{ 记 } b^2=b*b$$

$$b^2*b=b*b^2\in S, \text{ 记 } b^3=b^2*b=b*b^2$$

$$\vdots$$

因为 S 是有限集，所以必定存在 $j>i$，使得

$$b^i=b^j$$

令
$$p=j-i$$

便有
$$b^i=b^p*b^i$$

所以
$$b^q=b^p*b^q \qquad q\geq i$$

因为 $p\geq 1$，所以总可以找到 $k\geq 1$，使得

$$kp\geq i$$

对于 S 中的元素 b^{kp}，就有

$$\begin{aligned}b^{kp}&=b^p*b^{kp}\\&=b^p*(b^p*b^{kp})\\&=b^{2p}*b^{kp}\\&=b^{2p}*(b^p*b^{kp})\\&=\cdots\\&=b^{kp}*b^{kp}\end{aligned}$$

这就证明了在 S 中存在元素 $a=b^{kp}$，使得

$$a*a=a$$ □

定义 5-3.3 含有幺元的半群称为独异点。

例如，代数系统 $\langle R, +\rangle$ 是一个独异点，因为，$\langle R, +\rangle$ 是一个半群，且 0 是 R 中关于运算 $+$ 的幺元。另外，代数系统 $\langle I, \cdot\rangle$，$\langle I_+, \cdot\rangle$，$\langle R, \cdot\rangle$ 都是具有幺元 1 的半群，因此它们都是独异点。

可是，代数系统 $\langle N-\{0\}, +\rangle$ 虽是一个半群，但关于运算 $+$ 不存在幺元，所以，这个代数系统不是独异点。

定理 5-3.3 设 $\langle S, *\rangle$ 是一个独异点，则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的。

证明 设 S 中关于运算 $*$ 的幺元是 e。因为对于任意的 a，$b\in S$ 且 $a\neq b$ 时，总有

$$e*a=a\neq b=e*b$$

和

$$a*e=a\neq b=b*e$$

所以，在 $*$ 的运算表中不可能有两行或两列是相同的。 □

例题 4 设 I 是整数集合，m 是任意正整数，Z_m 是由模 m 的同余类组成的同余类集，在 Z_m 上定义两个二元运算 $+_m$ 和 $\times_m$ 分别如下：

对于任意的 $[i],[j]\in Z_m$

$$[i]+_m[j]=[(i+j)(\mathrm{mod}\ m)]$$

$$[i]\times_m[j]=[(i\times j)(\mathrm{mod}\ m)]$$

试证明在这两个二元运算的运算表中任何两行或两列都不相同。

证明 考察代数系统 $\langle Z_m, +_m\rangle$ 和 $\langle Z_m, \times_m\rangle$。

(1) 由运算 $+_m$ 和 $\times_m$ 的定义，可知它们在 Z_m 上都是封闭的。

(2) 对于任意 $[i],[j],[k]\in Z_m$

$$([i]+_m[j])+_m[k]=[i]+_m([j]+_m[k])$$
$$=[(i+j+k)(\mathrm{mod}\ m)]$$
$$([i]\times_m[j])\times_m[k]=[i]\times_m([j]\times_m[k])$$
$$=[(i\times j\times k)(\mathrm{mod}\ m)]$$

即 $+_m$，$\times_m$ 都是可结合的。

(3) 因为 $[0]+_m[i]=[i]+_m[0]=[i]$，所以，$[0]$ 是 $\langle Z_m, +_m\rangle$ 中的幺元。因为 $[1]\times_m[i]=[i]\times_m[1]=[i]$，所以 $[1]$ 是 $\langle Z_m, \times_m\rangle$ 中的幺元。

因此，代数系统$\langle Z_m, +_m\rangle$，$\langle Z_m, \times_m\rangle$都是独异点。由定理5-3.3可知，这两个运算的运算表中任何两行或两列都不相同。

上例中，如果给定$m=5$，那么，$+_5$和$\times_5$的运算表分别如表5-3.2和表5-3.3所示。

表 5-3.2

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

表 5-3.3

$\times_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

显然，上述运算表中没有两行或两列是相同的。

定理5-3.4 设$\langle S, *\rangle$是独异点，对于任意$a, b\in S$，且a，b均有逆元，则

a) $(a^{-1})^{-1}=a$

b) $a*b$有逆元，且$(a*b)^{-1}=b^{-1}*a^{-1}$

证明 a) 因为a^{-1}是a的逆元，即

$$a*a^{-1}=a^{-1}*a=e$$

所以
$$(a^{-1})^{-1}=a$$

b) 因为

$$(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}$$
$$=a*e*a^{-1}=a*a^{-1}=e$$

同理可证
$$(b^{-1}*a^{-1})*(a*b)=e$$

所以

$$(a*b)^{-1}=b^{-1}*a^{-1}$$ □

5-3 习题

(1) 对于正整数 k, $N_k=\{0, 1, 2, \cdots, k-1\}$, 设 $*_k$ 是 N_k 上的一个二元运算, 使得 $a*_k b=$用 k 除 $a\cdot b$ 所得的余数, 这里 $a, b\in N_k$。

a) 当 $k=4$ 时, 试造出 $*_k$ 的运算表。

b) 对于任意正整数 k, 证明 $\langle N_k, *_k\rangle$ 是一个半群。

(2) 设 $\langle S, *\rangle$ 是一个半群, $a\in S$, 在 S 上定义一个二元运算 □, 使得对于 S 中的任意元素 x 和 y, 都有

$$x \square y=x*a*y$$

证明二元运算 □ 是可结合的。

(3) 设 $\langle R, *\rangle$ 是一个代数系统, $*$ 是 R 上的一个二元运算, 使得对于 R 中的任意元素 a, b 都有

$$a*b=a+b+a\cdot b$$

证明 0 是幺元且 $\langle R, *\rangle$ 是独异点。

(4) 设 $X\neq\phi$, 令 $S=t(X)=\bigcup_{n=0}^{\infty}X^n$, 在 S 上定义二元运算 $\triangle$, 对任意 $\alpha=(x_1, x_2, \cdots, x_p)\in X^p$, $\beta=(y_1, y_2, \cdots, y_q)\in X^q$, 有

$$\alpha\triangle\beta=(x_1, x_2, \cdots, x_p, y_1, y_2, \cdots, y_q)\in X^{p+q}$$

证明 $\langle S, \triangle\rangle$ 是一个独异点。

(5) 设 $\langle A, *\rangle$ 是一个半群, 而且对于 A 中的元素 a 和 b, 如果 $a\neq b$ 必有 $a*b\neq b*a$, 试证明

a) 对于 A 中每个元素 a, 有 $a*a=a$

b) 对于 A 中任何元素 a 和 b, 有 $a*b*a=a$

c) 对于 A 中任何元素 a, b 和 c, 有 $a*b*c=a*c$

(6) 如果 $\langle S, *\rangle$ 是半群, 且 $*$ 是可交换的, 称 $\langle S, *\rangle$ 为可交换半群。证明: 如果 S 中有元素 a, b, 使得 $a*a=a$ 和 $b*b=b$, 则 $(a*b)*(a*b)=a*b$。

5-4 群与子群

定义 5-4.1 设 $\langle G, *\rangle$ 是一个代数系统, 其中 G 是非空集合, $*$ 是 G 上一个二元运算, 如果

(1) 运算 $*$ 是封闭的。

(2) 运算 $*$ 是可结合的。

(3) 存在幺元 e。

(4) 对于每一个元素 $x\in G$，存在着它的逆元 x^{-1}。

则称 $\langle G, *\rangle$ 是一个群。

例如，$\langle R-\{0\}, \times\rangle$，$\langle \mathscr{P}(S), \oplus\rangle$ 等都是群。

例题 1 设 $R=\{0°, 60°, 120°, 180°, 240°, 300°\}$ 表示在平面上几何图形绕形心顺时针旋转角度的六种可能情况，设 ★ 是 R 上的二元运算，对于 R 中任意两个元素 a 和 b，a★b 表示平面图形连续旋转 a 和 b 得到的总旋转角度。并规定旋转 360° 等于原来的状态，就看作没有经过旋转。验证 $\langle R$, ★$\rangle$ 是一个群。

解 由题意，R 上二元运算 ★ 的运算表如表 5-4.1 所示。

表 5-4.1

★	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

由表 5-4.1 可见，运算 ★ 在 R 上是封闭的。

对于任意的 $a, b, c\in R$，$(a$★$b)$★c 表示将图形依次旋转 a，b 和 c，而 a★$(b$★$c)$ 表示将图形依次旋转 b，c 和 a，而总的旋转角度都等于 $a+b+c \pmod{360°}$，因此，$(a$★$b)$★$c=a$★$(b$★$c)$。

0° 是幺元。

60°, 180°, 120° 的逆元分别是 300°, 180°, 240°。因此，$\langle R$, ★$\rangle$ 是一个群。

定义 5-4.2 设 $\langle G, *\rangle$ 是一个群。如果 G 是有限集，那么称 $\langle G, *\rangle$ 为有限群，G 中元素的个数通常称为该有限群的阶数，记为 $|G|$；如果 G 是无限集，则称 $\langle G, *\rangle$ 为无限群。

例题 1 中所述的 $\langle R$, ★$\rangle$ 就是一个有限群，且 $|R|=6$。

例题 2 试验证代数系统 $\langle I, +\rangle$ 是一个群，这里 I 是所有整数的集合，$+$ 是普通加法运算。

解　明显地，二元运算 + 在 I 上是封闭的且是可结合的。幺元是 0。对于任一 $a\in A$，它的逆元是 $-a$。所以 $\langle I,\ +\rangle$ 是一个群，且是一个无限群。

至此，我们可以概括地说：广群仅仅是一个具有封闭二元运算的非空集合；半群是一个具有结合运算的广群；独异点是具有幺元的半群；群是每个元素都有逆元的独异点。即有：

$$\{群\}\subset\{独异点\}\subset\{半群\}\subset\{广群\}$$

亦可由图 5-4.1 说明。

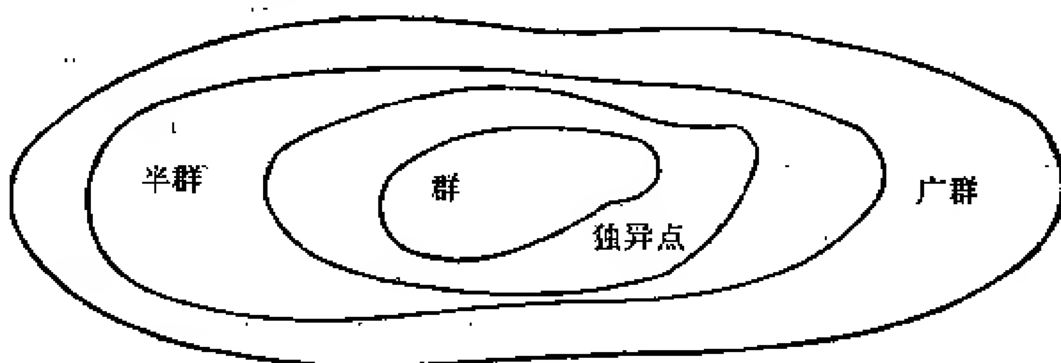


图　5-4.1

由定理 5-2.4 可知，群中任何一个元素的逆元必定是唯一的。由群中逆元的唯一性，我们可以有以下几个定理。

定理 5-4.1　群中不可能有零元。

证明　当群的阶为 1 时，它的唯一元素视作幺元。

设 $|G|>1$ 且群 $\langle G,\ *\rangle$ 有零元 θ。那么群中任何元素 $x\in G$，都有 $x*\theta=\theta*x=\theta\neq e$，所以，零元 θ 就不存在逆元，这与 $\langle G,\ *\rangle$ 是群相矛盾。□

定理 5-4.2　设 $\langle G,\ *\rangle$ 是一个群，对于 $a,\ b\in G$，必存在唯一的 $x\in G$，使得 $a*x=b$。

证明　设 a 的逆元是 a^{-1}，令

$$x=a^{-1}*b$$

则

$$\begin{aligned}a*x&=a*(a^{-1}*b)\\&=(a*a^{-1})*b\\&=e*b\\&=b\end{aligned}$$

若另有一解 x_1，满足 $a*x_1=b$，则

$$a^{-1}*(a*x_1)=a^{-1}*b$$

即

$$x_1=a^{-1}*b。$$

□

定理 5-4.3 设 $\langle G, *\rangle$ 是一个群，对于任意的 a，b，$c\in G$，如果有 $a*b=a*c$ 或者 $b*a=c*a$，则必有 $b=c$（消去律）。

证明 设 $a*b=a*c$，且 a 的逆元是 a^{-1}，则有

$$a^{-1}*(a*b)=a^{-1}*(a*c)$$

$$(a^{-1}*a)*b=(a^{-1}*a)*c$$

$$e*b=e*c$$

$$b=c$$

当 $b*a=c*a$ 时，可同样证得 $b=c$。 □

由定理 5-3.3 可知：群的运算表中没有两行（或两列）是相同的。为了进一步考察群的运算表所具有的性质，现在引进置换的概念。

定义 5-4.3 设 S 是一个非空集合，从集合 S 到 S 的一个双射称为 S 的一个置换。

譬如，对于集合 $S=\{a, b, c, d\}$，将 a 映射到 b，b 映射到 d，c 映射到 a，d 映射到 c 是一个从 S 到 S 上的一个一对一映射，这个置换可以表示为

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

即上一行中按任何次序写出集合中的全部元素，而在下一行中写每个对应元素的象。

定理 5-4.4 群 $\langle G, *\rangle$ 的运算表中的每一行或每一列都是 G 的元素的一个置换。

证明 首先，证明运算表中的任一行或任一列所含 G 中的一个元素不可能多于一次。用反证法，如果对应于元素 $a\in G$ 的那一行中有两个元素都是 c，即有

$$a*b_1=a*b_2=c, \quad 且\ b_1\neq b_2$$

由可约性可得 $b_1=b_2$，这与 $b_1\neq b_2$ 矛盾。

其次，要证明 G 中的每一个元素都在运算表的每一行和每一列中出现。考察对应于元素 $a\in G$ 的那一行，设 b 是 G 中的任一元素，由于 $b=a*(a^{-1}*b)$，所以 b 必定出现在对应于 a 的那一行中。

再由运算表中没有两行(或两列)相同的事实，便可得出：$\langle G, *\rangle$的运算表中每一行都是 G 的元素的一个置换，且每一行都是不相同的。同样的结论对于列也是成立的。 □

定义 5-4.4 代数系统 $\langle G, *\rangle$ 中，如果存在 $a\in G$，有 $a*a=a$，则称 a 为等幂元。

定理 5-4.5 在群 $\langle A, *\rangle$ 中，除幺元 e 外，不可能有任何别的等幂元。

证明 因为 $e*e=e$，所以 e 是等幂元。

现设 $a\in A,\ a\neq e$ 且 $a*a=a$

则有

$$a=e*a=(a^{-1}*a)*a=a^{-1}*(a*a)$$
$$=a^{-1}*a=e$$

与假设 $a\neq e$ 相矛盾。 □

下面介绍子群的概念。

定义 5-4.5 设 $\langle G, *\rangle$ 是一个群，S 是 G 的非空子集，如果 $\langle S, *\rangle$ 也构成群，则称 $\langle S, *\rangle$ 是 $\langle G, *\rangle$ 的一个子群。

定理 5-4.6 设 $\langle G, *\rangle$ 是一个群，$\langle S, *\rangle$ 是 $\langle G, *\rangle$ 的一个子群，那么，$\langle G, *\rangle$ 中的幺元 e 必定也是 $\langle S, *\rangle$ 中的幺元。

证明 设 $\langle S, *\rangle$ 中的幺元为 e_1，对于任一 $x\in S\subseteq G$，必有

$e_1*x=x=e*x$，故 $e_1=e$。 □

定义 5-4.6 设 $\langle G, *\rangle$ 是一个群，$\langle S, *\rangle$ 是 $\langle G, *\rangle$ 的子群，如果 $S=\{e\}$，或者 $S=G$，则称 $\langle S, *\rangle$ 为 $\langle G, *\rangle$ 的平凡子群。

例题 3 $\langle I, +\rangle$ 是一个群，设 $I_E=\{x|x=2n,\ n\in I\}$，证明 $\langle I_E, +\rangle$ 是 $\langle I, +\rangle$ 的一个子群。

证明 (1) 对于任意的 $x, y\in I_E$，不妨设 $x=2n_1, y=2n_2, n_1, n_2\in I$，则

$$x+y=2n_1+2n_2=2(n_1+n_2)$$

而 $$n_1+n_2\in I$$

所以 $$x+y\in I_E$$

即 + 在 I_E 上封闭。

(2) 运算+在 I_E 上保持可结合性。

(3) $\langle I, +\rangle$ 中的幺元 0 也在 I_E 中。

(4) 对于任意的 $x\in I_E$，必有 n 使得 $x=2n$，而

$$-x=-2n=2(-n),\ -n\in I$$

所以 $-x\in I_E$，而 $x+(-x)=0$，因此，$\langle I_E, +\rangle$ 是 $\langle I, +\rangle$ 的一个子群。

定理 5-4.7 设 $\langle G, *\rangle$ 是一个群，B 是 G 的非空子集，如果 B 是一个有限集，那么，只要运算 $*$ 在 B 上封闭，$\langle B, *\rangle$ 必定是 $\langle G, *\rangle$ 的子群。

证明 设 b 是 B 中的任一个元素。若 $*$ 在 B 上封闭，则元素 $b^2=b*b$，$b^3=b^2*b$，… 都在 B 中。由于 B 是有限集，所以必存在正整数 i 和 j，不妨假设 $i<j$，使得

$$b^i=b^j$$

即 $$b^i=b^i*b^{j-i}。$$

这就说明 b^{j-i} 是$\langle G, *\rangle$中的幺元，且这个幺元也在子集 B 中。

如果 $j-i>1$，那么由 $b^{j-i}=b*b^{j-i-1}$ 可知 b^{j-i-1} 是 b 的逆元，且 $b^{j-i-1}\in B$；如果 $j-i=1$，那么由 $b^i=b^i*b$ 可知 b 就是幺元，而幺元是以自身为逆元的。

因此，$\langle B, *\rangle$ 是 $\langle A, *\rangle$ 的一个子群。 □

例题 4 设 $G_4=\{p=\langle p_1, p_2, p_3, p_4\rangle \mid p_i\in\{0, 1\}\}$，$\oplus$ 是 G_4 上的二元运算，定义为，对任意 $X=\langle x_1, x_2, x_3, x_4\rangle$，$Y=\langle y_1, y_2, y_3, y_4\rangle\in G_4$

$$X\oplus Y=\langle x_1\bar{\vee} y_1,\ x_2\bar{\vee} y_2,\ x_3\bar{\vee} y_3,\ x_4\bar{\vee} y_4\rangle$$

其中 $\bar{\vee}$ 的运算表如表 5-4.2 所示。

证明 $\langle\{\langle 0, 0, 0, 0\rangle, \langle 1, 1, 1, 1\rangle\}, \oplus\rangle$ 是群 $\langle G_4, \oplus\rangle$ 的子群。

表 5-4.2

$\bar{\vee}$	0	1
0	0	1
1	1	0

证明　首先对于任意的 $X=\langle x_1, x_2, x_3, x_4\rangle$, $Y=\langle y_1, y_2, y_3, y_4\rangle$, $Z=\langle z_1, z_2, z_3, z_4\rangle\in G_4$。

因为
$$x_i\overline{\nabla} y_i\in\{0, 1\}$$
所以
$$X\oplus Y\in G_4$$
因为
$$(x_i\overline{\nabla} y_i)\overline{\nabla} z_i=x_i\overline{\nabla}(y_i\overline{\nabla} z_i)$$
所以
$$(X\oplus Y)\oplus Z=X\oplus(Y\oplus Z)$$

$\langle 0, 0, 0, 0\rangle$ 是幺元。

$X\oplus X=\langle 0, 0, 0, 0\rangle$，即任一 X，以它自身为逆元。

所以，$\langle G_4, \oplus\rangle$ 是一个群。

其次，由于 $\{\langle 0, 0, 0, 0\rangle, \langle 1, 1, 1, 1\rangle\}\subset G_4$，且 $\oplus$ 在 $\{\langle 0, 0, 0, 0\rangle, \langle 1, 1, 1, 1\rangle\}$ 上是封闭的，由定理 5-4.7 可知 $\langle\{\langle 0, 0, 0, 0\rangle, \langle 1, 1, 1, 1\rangle\}, \oplus\rangle$ 是 $\langle G_4, \oplus\rangle$ 的子群。

定理 5-4.8　设 $\langle G, \triangle\rangle$ 是群，S 是 G 的非空子集，如果对于 S 中的任意元素 a 和 b 有 $a\triangle b^{-1}\in S$，则 $\langle S, \triangle\rangle$ 是 $\langle G, \triangle\rangle$ 的子群。

证明　首先证明，G 中的幺元 e 也是 S 中的幺元。

任取 S 中的元素 a，$a\in S\subset G$，所以 $e=a\triangle a^{-1}\in S$ 且 $a\triangle e=e\triangle a=a$，即 e 也是 S 中的幺元。

其次证明，S 中的每一元素都有逆元。

对任一 $a\in S$，因为 $e\in S$，所以，$e\triangle a^{-1}\in S$ 即 $a^{-1}\in S$。

最后证明，$\triangle$ 在 S 上是封闭的。

对任意的 a, $b\in S$，由上可知 $b^{-1}\in S$

而
$$b=(b^{-1})^{-1}$$
所以
$$a\triangle b=a\triangle(b^{-1})^{-1}\in S$$

至于，运算 $\triangle$ 在 S 上的可结合性是保持的。因此，$\langle S, \triangle\rangle$ 是 $\langle G, \triangle\rangle$ 的子群。　□

例题 5　设 $\langle H, *\rangle$ 和 $\langle K, *\rangle$ 都是群 $\langle G, *\rangle$ 的子群，试证明 $\langle H\cap K, *\rangle$ 也是 $\langle G, *\rangle$ 的子群。

证明　设任意的 a, $b\in H\cap K$，因为 $\langle H, *\rangle$ 和 $\langle K, *\rangle$ 都是子群，所以 $b^{-1}\in H\cap K$，由于 $*$ 在 H 和 K 中的封闭性，所以 $a*b^{-1}\in H\cap K$，由定理 5-4.8 即得 $\langle H\cap K, *\rangle$ 是 $\langle G, *\rangle$ 的子群。

5-4 习题

(1) 设 $X=R-\{0, 1\}$，在 X 上定义 6 个函数如下：

对于任意 $x\in X$,

$$f_1(x)=x;\ f_2(x)=x^{-1};\ f_3(x)=1-x$$

$$f_4(x)=(1-x)^{-1};\ f_5(x)=(x-1)x^{-1};\ f_6(x)=x(x-1)^{-1}$$

试证明 $\langle F, \circ\rangle$ 是一个群。其中 $F=\{f_1, f_2, f_3, f_4, f_5, f_6\}$，$\circ$ 是函数的复合运算。

(2) 设 $\langle A, *\rangle$ 是半群，e 是左幺元且对每一个 $x\in A$，存在 $\hat{x}\in A$，使得 $\hat{x}*x=e$。

a) 证明：对于任意的 $a, b, c\in A$，如果 $a*b=a*c$，则 $b=c$。

b) 通过证明 e 是 A 中的幺元，证明 $\langle A, *\rangle$ 是群。

(3) 设 $\langle G, *\rangle$ 是群，对任一 $a\in G$，令 $H=\{y|y*a=a*y, y\in G\}$，试证明 $\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的子群。

(4) 设 $\langle H, \cdot\rangle$ 和 $\langle K, \cdot\rangle$ 都是群 $\langle G, \cdot\rangle$ 的子群，令

$$HK=\{h\cdot k|h\in H, k\in K\}$$

证明：$\langle HK, \cdot\rangle$ 是 $\langle G, \cdot\rangle$ 的子群的充要条件是 $HK=KH$。

(5) 设 $\langle A, *\rangle$ 是群，且 $|A|=2n$，$n\in N$。证明：在 A 中至少存在 $a\neq e$，使得 $a*a=e$。其中 e 是幺元。

5-5 阿贝尔群和循环群

定义 5-5.1 如果群 $\langle G, *\rangle$ 中的运算 $*$ 是可交换的，则称该群为阿贝尔群，或称交换群。

例题 1 设 $S=\{a, b, c, d\}$，在 S 上定义一个双射函数 f：$f(a)=b$，$f(b)=c$，$f(c)=d$，$f(d)=a$，对于任一 $x\in S$，构造复合函数

$$f^2(x)=f\circ f(x)=f(f(x))$$

$$f^3(x)=f\circ f^2(x)=f(f^2(x))$$

$$f^4(x)=f\circ f^3(x)=f(f^3(x))$$

如果用 f^0 表示 S 上的恒等映射，即

$$f^0(x)=x \qquad x\in S$$

很明显地有 $f^4(x)=f^0(x)$，记 $f^1=f$，构造集合 $F=\{f^0, f^1, f^2, f^3\}$，那么 $\langle F, \circ\rangle$ 是一个阿贝尔群。

解 对于 F 中任意两个函数的复合，可以由表 5-5.1 给出。

表 5-5.1

$\circ$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^0	f^3	f^2
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^2	f^1	f^0

可见，复合运算 $\circ$ 关于 F 是封闭的，并且是可结合的。

f^0 是关于复合运算 $\circ$ 的幺元。

f^0 的逆元就是它自身，f^1 和 f^3 互为逆元，f^0 的逆元也是它自身。

由表 5-5.1 的对称性，可知复合运算 $\circ$ 是可交换的。因此，$\langle F, \circ\rangle$ 是一个阿贝尔群。

例题 2 设 G 为所有 n 阶非奇（满秩）矩阵的集合，矩阵乘法运算 $\circ$ 作为定义在集合 G 上的二元运算，则 $\langle G, \circ\rangle$ 是一个不可交换群。

解 任意两个 n 阶非奇矩阵相乘后，仍是一个非奇矩阵，所以运算 $\circ$ 是封闭的。

矩阵乘法运算是可结合的。

n 阶单位阵 E 是 G 中的幺元。

任意一个非奇阵 A 存在着唯一的逆阵 A^{-1}，使

$$A^{-1}\circ A=A\circ A^{-1}=E。$$

但矩阵乘法是不可交换的，因此，$\langle G, \circ\rangle$ 是一个不可交换群。

定理 5-5.1 设 $\langle G, *\rangle$ 是一个群，$\langle G, *\rangle$ 是阿贝尔群的充要条件是对任意的 $a, b\in G$，有 $(a*b)*(a*b)=(a*a)*(b*b)$。

证明 充分性

设对任意 $a, b\in G$，有

$$(a*b)*(a*b)=(a*a)*(b*b)$$

因为
$$\begin{aligned} a*(a*b)*b&=(a*a)*(b*b)\\ &=(a*b)*(a*b)\\ &=a*(b*a)*b \end{aligned}$$

所以 $$a^{-1}*(a*(a*b)*b)*b^{-1}=a^{-1}*(a*(b*a)*b)*b^{-1}$$

即得 $$a*b=b*a$$

因此，群 $\langle G, *\rangle$ 是阿贝尔群。

必要性

设 $\langle G, *\rangle$ 是阿贝尔群，则对任意的 $a, b\in G$，有

$$a*b=b*a$$

因此
$$\begin{aligned}(a*a)*(b*b)&=a*(a*b)*b\\&=a*(b*a)*b\\&=(a*b)*(a*b)\end{aligned}$$
□

定义 5-5.2 设 $\langle G, *\rangle$ 为群，若在 G 中存在一个元素 a，使得 G 中的任意元素都由 a 的幂组成，则称该群为循环群，元素 a 称为循环群 G 的生成元。

例如，$60°$ 就是群 $\langle\{0°, 60°, 120°, 180°, 240°, 300°\}, ★\rangle$ 的生成元，因此，该群是循环群。

定理 5-5.2 任何一个循环群必定是阿贝尔群。

证明 设 $\langle G, *\rangle$ 是一个循环群，它的生成元是 a，那么，对于任意的 $x, y\in G$，必有 $r, s\in I$，使得

$$x=a^r \quad 和 \quad y=a^s$$

而且
$$x*y=a^r*a^s=a^{r+s}=a^{s+r}=a^s*a^r=y*x$$

因此，$\langle G, x\rangle$ 是一个阿贝尔群。 □

对于有限循环群，有下面的定理。

定理 5-5.3 设 $\langle G, *\rangle$ 是一个由元素 $a\in G$ 生成的有限循环群。如果 G 的阶数是 n，即 $|G|=n$，则 $a^n=e$，且

$$G=\{a, a^2, a^3, \cdots, a^{n-1}, a^n=e\}$$

其中，e 是 $\langle G, *\rangle$ 中的幺元，n 是使 $a^n=e$ 的最小正整数（称 n 为元素 a 的阶）。

证明 假设对于某个正整数 m，$m<n$，有 $a^m=e$。那么，由于 $\langle G, *\rangle$ 是一个循环群，所以 G 中的任何元素都能写为 $a^k(k\in I)$，而且 $k=mq+r$，其中，q 是某个整数，$0\leqslant r<m$。这就有

$$a^k=a^{mq+r}=(a^m)^q*a^r=a^r$$

这就导致 G 中每一个元素都可表示成 $a^r(0\leqslant r<m)$，这样，G 中最多有 m 个不同的元素，与 $|G|=n$ 相矛盾。所以 $a^m=e(m<n)$ 是不可能的。

进一步证明 $a, a^2, \cdots, a^n$ 都不相同。用反证法。假设 $a^i=a^j$，其中 $1\leqslant i<j\leqslant n$，就有 $a^{j-i}=e$，而且 $1\leqslant j-i<n$，这已经由上面证明是不可能的。所以，$a, a^2, \cdots, a^n$ 都不相同，因此

$$G=\{a, a^2, a^3, \cdots, a^n=e\}$$ □

例题 3 设 $G=\{\alpha, \beta, \gamma, \delta\}$，在 G 上定义二元运算 $*$ 如表 5-5.2 所示。

表 5-5.2

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

说明 $\langle G, *\rangle$ 是一个循环群。

解　由运算表 5-5.2 可知运算 $*$ 是封闭的，α 是幺元。β, γ 和 δ 的逆元分别是 β, δ 和 γ。可以验证运算 $*$ 是可结合的。所以 $\langle G, *\rangle$ 是一个群。

在这个群中，由于

$$\gamma*\gamma=\gamma^2=\beta,\quad \gamma^3=\delta,\quad \gamma^4=\alpha$$

以及

$$\delta*\delta=\delta^2=\beta,\ \delta^3=\gamma,\ \delta^4=\alpha$$

故群 $\langle G, *\rangle$ 是由 γ 或 δ 生成的，因此 $\langle G, *\rangle$ 是一个循环群。

从例题 3 中可以看到：一个循环群的生成元可以不是唯一的。

5-5 习题

(1) 设 $\langle G, *\rangle$ 是一个独异点，并且对于 G 中的每一个元素 x 都有 $x*x=e$，其中 e 是幺元，证明 $\langle G, *\rangle$ 是一个阿贝尔群。

(2) 证明任何阶数分别为 1，2，3，4 的群都是阿贝尔群。并举一个 6 阶群，它不是阿贝尔群。

(3) 设 $\langle G, *\rangle$ 是一个群，证明：如果对任意的 $a, b\in G$ 都有 $a^3*b^3=(a*b)^3$，$a^4*b^4=(a*b)^4$ 和 $a^5*b^5=(a*b)^5$，则 $\langle G, *\rangle$ 是一个阿贝尔群。

(4) 设 $G=\{[1], [2], [3], [4], [5], [6]\}$，$G$ 上的二元运算 $\times_7$ 如表 5-5.3 所示。

问 $\langle G, \times_7\rangle$ 是循环群吗？若是，试找出它的生成元。

(5) 证明：循环群的任何子群必定也是循环群。

表 5-5.3

$\times_7$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

*5-6 置换群与伯恩赛德定理

在这一节中，我们将讨论另一类重要的群——置换群。

对于一个具有 n 个元素的集合 S，将 S 上所有 $n!$ 个不同置换所组成的集合记作 S_n。

定义 5-6.1 设 $\pi_1, \pi_2 \in S_n$，S_n 上的二元运算 $\circ$ 和 $\diamondsuit$，使得 $\pi_1 \circ \pi_2$ 和 $\pi_2 \diamondsuit \pi_1$ 都表示对 S 的元素先应用置换 π_2 接着再应用置换 π_1 所得到的置换。二元运算 $\circ$ 和 $\diamondsuit$ 分别称为左复合和右复合。

例 1 设 $S=\{a, b, c, d\}$，S_4 中的两个元素

$$\pi_1=\begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}, \quad \pi_2=\begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$$

则

$$\begin{aligned}\pi_1 \circ \pi_2 = \pi_2 \diamondsuit \pi_1 &= \begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} \\ &= \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}\end{aligned}$$

为确定起见，我们在下面只对左复合进行讨论。

定理 5-6.1 $\langle S_n, \circ \rangle$ 是一个群，其中 $\circ$ 是置换的左复合运算。

证明 首先证明二元运算$\circ$在S_n上的封闭性。

对于任意的π_1, $\pi_2 \in S_n$, 如果a, $b \in S$且$a \neq b$, 那么, 当π_2将a, b分别映照成c, $d \in S$时, 必定有$c \neq d$; 同样地, 当π_1将c, d分别映照成e, $f \in S$时, 必定有$e \neq f$, 于是, $\pi_1 \circ \pi_2$必定将S中任意两个不同元素映照到S中的两个不同元素。因此, $\pi_1 \circ \pi_2 \in S_n$。

其次, 证明二元运算$\circ$在S_n上是可结合的。

对于任意的π_1, π_2, $\pi_3 \in S_n$, 如果对任一$x \in S$, 有$\pi_3(x)=y$, $\pi_2(y)=z$, $\pi_1(z)=\omega$, 那么, 由于

$$\pi_1 \circ \pi_2(y)=\pi_1(\pi_2(y))=\pi_1(z)=\omega$$

所以 $$(\pi_1 \circ \pi_2) \circ \pi_3(x)=(\pi_1 \circ \pi_2)(\pi_3(x))=(\pi_1 \circ \pi_2)(y)=\omega$$

同样地, 由于 $$\pi_2 \circ \pi_3(x)=\pi_2(\pi_3(x))=\pi_2(y)=z$$

所以 $$\pi_1 \circ (\pi_2 \circ \pi_3)(x)=\pi_1(\pi_2 \circ \pi_3(x))=\pi_1(z)=\omega$$

因此 $$\pi_1 \circ (\pi_2 \circ \pi_3)=(\pi_1 \circ \pi_2) \circ \pi_3$$

如果将S中的每个元素映照到它自身的那个置换, 记作π_e, 那么对于任一$\pi_x \in S_n$都有, $\pi_e \circ \pi_x=\pi_x \circ \pi_e=\pi_x$, 因此, S_n中存在幺元π_e, 称它为幺置换。

最后, 对于任意的$\pi \in S_n$, 必定存在着对应的$\pi^{-1} \in S_n$, 使得如果π将$x \in S$映照到y, 那么π^{-1}将y映照到x, 因此

$$\pi \circ \pi^{-1}=\pi^{-1} \circ \pi=\pi_e$$ □

定义 5-6.2 $\langle S_n, \circ \rangle$的任何一个子群, 称为集合$S$上的一个置换群。特别地, 置换群$\langle S_n, \circ \rangle$称为集合$S$的对称群。

例题 1 设$S=\{1, 2, 3\}$, 写出S的对称群以及S上的置换群。

解 S的对称群为$\langle S_3, \circ \rangle$。

$$S_3=\{\pi_e, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5\}$$

其中, π_e, π_1, π_2, π_3, π_4, π_5如图 5-6.1 所示。S_3上的复合运算$\circ$如表 5-6.1 所示。

容易看出, $\langle \{\pi_e, \pi_1\}, \circ \rangle$, $\langle \{\pi_e, \pi_2\}, \circ \rangle$, $\langle \{\pi_e, \pi_3\}, \circ \rangle$和$\langle \{\pi_e, \pi_4, \pi_5\}, \circ \rangle$都是$\langle S_3, \circ \rangle$的子群, 即都是$S$上的置换群。

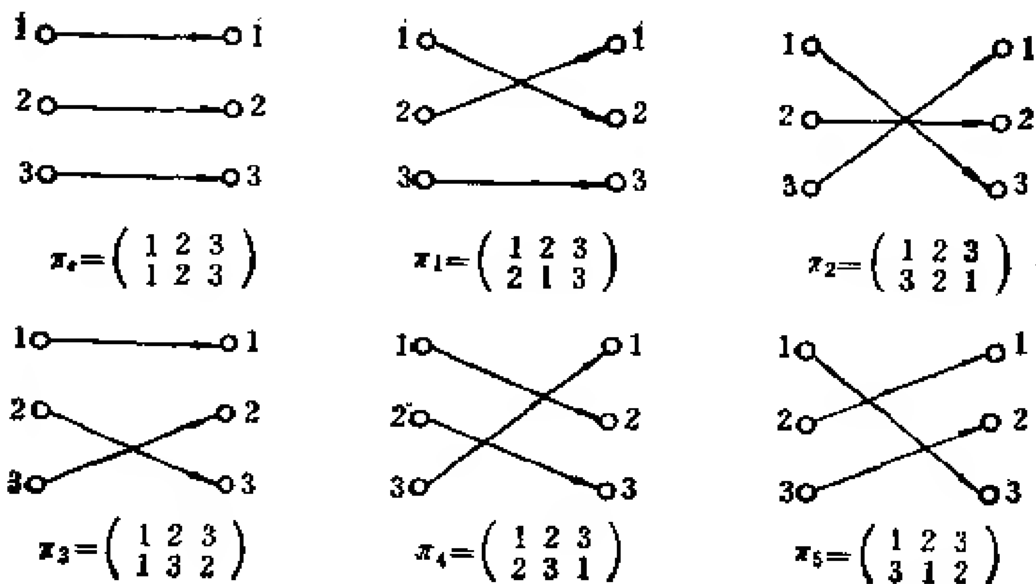


图 5-6.1

表 5-6.1

$\circ$	π_e	π_1	π_2	π_3	π_4	π_5
π_e	π_e	π_1	π_2	π_3	π_4	π_5
π_1	π_1	π_e	π_5	π_4	π_3	π_2
π_2	π_2	π_4	π_e	π_5	π_1	π_3
π_3	π_3	π_5	π_4	π_e	π_2	π_1
π_4	π_4	π_2	π_3	π_1	π_5	π_e
π_5	π_5	π_3	π_1	π_2	π_e	π_4

定义 5-6.3 设 $\langle G, \circ\rangle$ 是 S 的一个置换群，称

$$R=\{\langle a, b\rangle \mid \pi(a)=b,\ \pi\in G\}$$

为由 $\langle G, \circ\rangle$ 所诱导的 S 上的二元关系。

例 2 设 $S=\{a, b, c, d\}$，$G=\{\pi_e, \pi_1, \pi_2, \pi_3\}$，其中

$$\pi_e=\begin{pmatrix}a&b&c&d\\a&b&c&d\end{pmatrix},\quad \pi_1=\begin{pmatrix}a&b&c&d\\b&a&c&d\end{pmatrix}$$

$$\pi_2=\begin{pmatrix}a&b&c&d\\a&b&d&c\end{pmatrix},\quad \pi_3=\begin{pmatrix}a&b&c&d\\b&a&d&c\end{pmatrix}$$

容易验证 $\langle G, \circ\rangle$ 是 S 的一个置换群。而由 $\langle G, \circ\rangle$ 诱导的 S 上的二元关系可以由图 5-6.2 所示。



图 5-6.2

定理 5-6.2 由置换群 $\langle G, \circ\rangle$ 诱导的 S 上的二元关系是一个等价关系。

证明 $\langle G, \circ\rangle$ 诱导的 S 上的二元关系为

$$R=\{\langle a, b\rangle \mid \pi(a)=b, \pi\in G\}$$

因为幺置换 $\pi_e\in G$，所以对任一 $x\in S$，必有 $\langle x, x\rangle\in R$；设 $\langle a, b\rangle\in R$，则必有 $\pi\in G$，使得 $\pi(a)=b$，由于 $\langle G, \circ\rangle$ 是一个群，所以 $\pi^{-1}\in G$，即有 $\langle b, a\rangle\in R$；设 $\langle a, b\rangle\in R$ 和 $\langle b, c\rangle\in R$，则必有 π_1 和 $\pi_2\in G$，使得 $\pi_1(a)=b$ 和 $\pi_2(b)=c$，因为 $\pi_2\circ\pi_1\in G$，而 $\pi_2\circ\pi_1(a)=\pi_2(\pi_1(a))=\pi_2(b)=c$，即有 $\langle a, c\rangle\in R$。因此，R 是 S 上的一个等价关系。 □

我们知道，一个集合上的等价关系可以确定该集合的一个划分，这个划分中的每一块都是一个等价类。

给定一个集合 S 以及 S 上的一个置换群 $\langle G, \circ\rangle$，由 $\langle G, \circ\rangle$ 诱导的 S 上的等价关系 R 必将产生 S 的一个划分，我们常常要计算划分中等价类的数目。伯恩赛德(Burnside)提出了一种计算等价类数目的方法。为此，我们先介绍有关置换作用下不变元的概念。

定义 5-6.4 如果一个置换将一个元素映照到它自身，那么，这个元素就称为在这个置换作用下的不变元。用 $\psi(\pi)$ 表示在置换 π 作用下的不变元个数。

例如，置换

$$\pi_e=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

作用下的不变元为 a, b, c, d，$\psi(\pi_e)=4$。

$$\pi_1=\begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$$

作用下的不变元为 $c, d, \psi(\pi_1)=2$。

定理 5-6.3(伯恩赛德定理) 由 S 的置换群 $\langle G, \circ\rangle$ 诱导的等价关系将 S 划分所得的等价类数目等于

$$\frac{1}{|G|}\sum_{\pi\in G}\psi(\pi)$$

证明 首先，对于任一 $s\in S$，设 $\eta(s)$ 表示 G 中使 s 不变的置换个数。由于 $\sum_{\pi\in G}\psi(\pi)$ 和 $\sum_{s\in S}\eta(s)$ 都是 G 中置换作用下的不变元总数，因此

$$\sum_{\pi\in G}\psi(\pi)=\sum_{s\in S}\eta(s)$$

其次，设 a 和 b 是属于同一等价类的 S 中的两个元素，则可证明在 G 中恰存在 $\eta(a)$ 个将 a 映照到 b 的置换。为此，我们设

$$X_a=\{\pi_x|\pi_x(a)=a \text{ 且 } \pi_x\in G\}$$

显然，$|X_a|=\eta(a)$。因为 a, b 在同一等价类中，所以必存在一个置换 $\pi_t\in G$，使得

$$\pi_t(a)=b$$

构造集合 $X_t=\{\pi_t\circ\pi_x|\pi_x\in X_a\}$，那么，$X_t$ 中的每一个元素都是将元素 a 映照到元素 b 的置换。对于任意的 π_i, $\pi_j\in X_a$，如果

$$\pi_t\circ\pi_i=\pi_t\circ\pi_j,$$

必有 $\pi_t^{-1}\circ(\pi_t\circ\pi_i)=\pi_t^{-1}\circ(\pi_t\circ\pi_j)$，即 $\pi_i=\pi_j$，所以，X_t 中的置换都不相同；故有 $|X_t|=|X_a|=\eta(a)$。还可证明，除了 X_t 中的置换外，在 G 中不可能有别的置换能将 a 映照到 b 了，这是因为：假设另有一个置换 $\pi_y\in G$ 且 $\pi_y(a)=b$，那么由

$$\pi_t^{-1}(\pi_y(a))=\pi_t^{-1}(b)=a$$

可知，$\pi_t^{-1}\circ\pi_y\in X_a$，就有

$$\pi_t\circ(\pi_t^{-1}\circ\pi_y)\in X_t \quad \text{即} \quad \pi_y\in X_t$$

因此，在 G 中恰有 $\eta(a)$ 个置换将 a 映照到 b。

最后，设 $a, b, c, \cdots, h$ 是 S 中属于同一等价类的元素，于是在 G 的每一个置换中，a 只能映照到其所属等价类中的某一个元素，因此，我们只能将 G 中的所有置换分为以下各类：将 a 映照

到 a 的类；将 a 映照到 b 的类；…；将 a 映照到 h 的类。每一类中恰有 $\eta(a)$ 个置换，所以，我们有

$$\eta(a)=\frac{|G|}{\text{包含 } a \text{ 的等价类中元素的个数}}$$

同理可得

$$\eta(b)=\eta(c)=\cdots=\eta(h)=\frac{|G|}{\text{包含 } a \text{ 的等价类中元素的个数}}$$

因此，对于 S 中的任何一个等价类，我们有

$$\sum_{s\in\text{该等价类}}\eta(s)=|G|$$

由此可得

$$\sum_{s\in S}\eta(s)=(\text{划分}S\text{所得的等价类数目})\times|G|$$

因此

$$\text{划分 } S \text{ 所得的等价类数目}=\frac{1}{|G|}\sum_{s\in S}\eta(s)=\frac{1}{|G|}\sum_{\pi\in G}\psi(\pi)\quad\square$$

例题2 在一张卡片上打印一个十进制的5位数，对于小于10000的数，前面用零补足5位。如果一个数可以倒转过来读，例如89166，倒转过来读就是99168，就合用一张卡片。问共需多少张卡片才能打印所有的十进制5位数？

解 设 S 是所有十进制5位数的集合。根据题意，构造 S 的一个置换群 $\langle\{\pi_1,\pi_2\},\circ\rangle$，其中 π_1 是幺置换；π_2 是这样的一个置换：当一个数倒转过来不可读时，这个置换将该数映照到它自身，例如，将数16764映照成16764；当一个数倒转过来可读时，π_2 就将该数映照成倒转过来的数，例如，将数89198映照成86168。

因为，仅含有0，1，6，8，9的5位数是倒转可读的。共有 5^5 个，而其中还有那些以0，1，8居中，第一位数与第五位数互为倒转，第二位数与第四位数互为倒转的5位数，它们倒转过来还是自身，共有 3×5^2 个。所以，

$$\psi(\pi_2)=10^5-5^5+3\times5^2$$

另外 $\psi(\pi_1)=10^5$。

因此，共需卡片的张数为：

$$\frac{1}{2}(10^5+10^5-5^5+3\times5^2)=10^5-\frac{1}{2}\times5^5+\frac{3}{2}\times5^2$$

例题3 考察从蓝、黄、白三种颜色的珠子中遴取5粒串成的手镯，如果将一只手镯经过顺时针旋转而得到另一只手镯看作是没有区别的手镯，并称

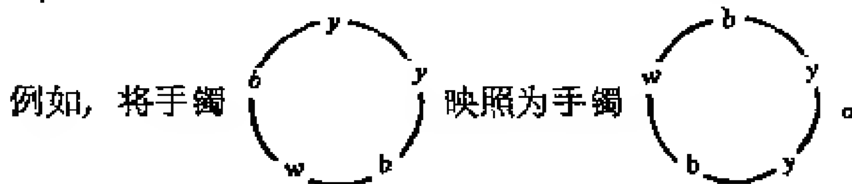
这两只手镯是旋转等价的，那么，在考虑旋转等价的条件下，不同手镯的数目是多少？

解　设 S 是不考虑旋转等价时所有用 5 粒珠子串成的手镯的集合，显然

$$|S|=3^5=243$$

手镯的旋转方式可以有：不旋转，顺时针旋转 1 粒珠子、2 粒珠子、3 粒珠子、4 粒珠子。旋转 5 粒珠子看作是没有旋转。

设 $S_1=\{\pi_e, \pi_1, \pi_2, \pi_3, \pi_4\}$，构造一个代数系统 $\langle S_1, \circ\rangle$，其中 π_e 是幺置换；π_1 这个置换是将一只手镯映照为按顺时针旋转 1 粒珠子而得到的手镯。



至于 π_2、π_3 和 π_4 是这样一些置换，它们分别将一只手镯映照为按顺时针旋转 2、3 和 4 粒珠子而得到的手镯。$\circ$ 是置换的复合，因为 S_1 对运算 $\circ$ 是封闭的，所以，代数系统 $\langle S_1, \circ\rangle$ 构成 S 的置换群。

我们知道，对于任何的手镯，当珠子颜色相同时，任意旋转都是保持不变的。当手镯中珠子粒数是质数时，那么，不可能有不同色的手镯保持旋转不变。本例中 5 是质数，所以只有全白、全蓝、全黄这三种手镯是旋转不变的，故 $\psi(\pi_4)=\psi(\pi_3)=\psi(\pi_2)=\psi(\pi_1)=3$，另外，$\psi(\pi_e)=243$。

因此，在考虑旋转等价的条件下，不同手镯的数目应是

$$\frac{1}{5}(243+3+3+3+3)=51$$

利用不同手镯数目的计算结果，可以直接地获得数论中有名的费尔马(Fermat)小定理的一个很有趣的证明。

对于质数 p，考察从 a 种不同颜色的珠子中选取 p 粒串成的手镯，在考虑旋转等价的条件下，不同手镯的数目应是

$$\frac{1}{p}(a^p+\overbrace{a+a+\cdots+a}^{p-1})=\frac{1}{p}(a^p+(p-1)a)$$

由于手镯的数目总是整数，所以 p 必须整除 a^p-a，即 p 必定能或者整除 a 或者整除 $a^{p-1}-1$，这正是费尔马小定理的结论。

5-6　习题

(1) 设有 $\{a, b, c, d, e\}$ 的置换如下：

$$\alpha=\begin{pmatrix} a & b & c & d & e \\ b & c & a & d & e \end{pmatrix} \quad \beta=\begin{pmatrix} a & b & c & d & e \\ a & b & c & e & d \end{pmatrix}$$

$$\gamma=\begin{pmatrix} a & b & c & d & e \\ e & d & c & b & a \end{pmatrix} \quad \delta=\begin{pmatrix} a & b & c & d & e \\ c & b & a & e & d \end{pmatrix}$$

试求 $\alpha\circ\beta$, $\beta\circ\alpha$, $\alpha\circ\alpha$, $\gamma\circ\beta$, δ^{-1}, $\alpha\circ\beta\circ\gamma$, 并解方程 $\alpha\circ x=\beta$, $y\circ\gamma=\delta$。

(2) 设 p 是质数，证明从 a 种颜色不同的珠子中选取 p 粒串成手镯，只有同色手镯保持旋转不变。

(3) 哪些对称群是阿贝尔群?

(4) 用 4 种不同颜色中的一种或几种来涂一根六节的棍棒，问有多少种不同的涂法?

(5) a) 2×2的棋盘，用白色或黑色涂在每一个方格内，在考虑旋转等价的条件下，试确定每个方格涂上颜色的不同棋盘的数目。

*b) 对于 4×4 的棋盘呢?

5-7 陪集与拉格朗日定理

现在，我们来讨论群理论中的又一重要内容：群 $\langle G, *\rangle$ 的任意子群 $\langle H, *\rangle$ 将 G 分解成 H 在 G 中的陪集。

定义 5-7.1 设 $\langle G, *\rangle$ 是一个群，A, $B\in\mathscr{P}(G)$ 且 $A\neq\emptyset$, $B\neq\emptyset$, 记

$$AB=\{a*b\mid a\in A,\ b\in B\}$$

和

$$A^{-1}=\{a^{-1}\mid a\in A\}$$

分别称为 A, B 的积和 A 的逆。

定义 5-7.2 设 $\langle H, *\rangle$ 是群 $\langle G, *\rangle$ 的一个子群，$a\in G$, 则集合 $\{a\}H\,(H\{a\})$ 称为由 a 所确定的 H 在 G 中的左陪集（右陪集），简称为 H 关于 a 的左陪集（右陪集），记为 aH (Ha)。元素 a 称为陪集 $aH\,(Ha)$ 的代表元素。

为确定起见，我们下面只对左陪集进行讨论。

例1 设 $G=R\times R$, R 为实数集，G 上的一个二元运算+定义为

$$\langle x_1, y_1\rangle+\langle x_2, y_2\rangle=\langle x_1+x_2, y_1+y_2\rangle$$

显然，$\langle G, +\rangle$ 是一个具有幺元 $\langle 0, 0\rangle$ 的阿贝尔群。

设 $$H=\{\langle x, y\rangle \mid y=2x\}$$

那么，很容易验证 $\langle H, +\rangle$ 是 $\langle G, +\rangle$ 的子群。对于 $\langle x_0, y_0\rangle \in G$，$H$ 关于 $\langle x_0, y_0\rangle$ 的左陪集为 $\langle x_0, y_0\rangle H$。这个例子的几何意义为：$G$ 是笛卡尔平面，H 是通过原点的直线 $y=2x$，陪集 $\langle x_0, y_0\rangle H$ 是通过点 $\langle x_0, y_0\rangle$ 且平行于 H 的直线。如图 5-7.1 所示：

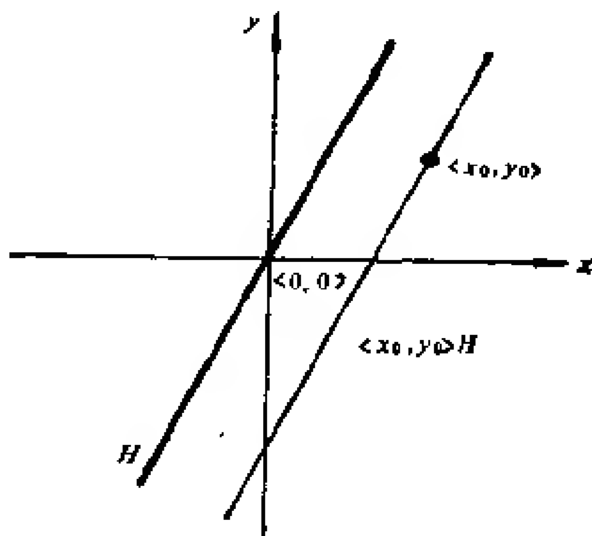


图 5-7.1

对于有限群，有下面一个很重要的结论。

定理 5-7.1 （拉格朗日定理） 设 $\langle H, *\rangle$ 是群 $\langle G, *\rangle$ 的一个子群，那么

(a) $R=\{\langle a, b\rangle \mid a\in G, b\in G$ 且 $a^{-1}*b\in H\}$ 是 G 中的一个等价关系。对于 $a\in G$，若记 $[a]_R=\{x \mid x\in G$ 且 $\langle a, x\rangle\in R\}$ 则

$$[a]_R=aH$$

(b) 如果 G 是有限群，$|G|=n$，$|H|=m$，则 $m\mid n$。

证明 (a) 对于任一 $a\in G$，必有 $a^{-1}\in G$，使 $a^{-1}*a=e\in H$，所以 $\langle a, a\rangle\in R$。

若 $\langle a, b\rangle\in R$，则 $a^{-1}*b\in H$，因为 H 是 G 的子群，故

$$(a^{-1}*b)^{-1}=b^{-1}*a\in H$$

所以，$\langle b, a\rangle\in R$。

若 $\langle a, b\rangle\in R$，$\langle b, c\rangle\in R$，则 $a^{-1}*b\in H$，$b^{-1}*c\in H$，所以 $a^{-1}*b*b^{-1}*c=a^{-1}*c\in H$，$\langle a, c\rangle\in R$。这就证明了 R 是 G 中的一个等价关系。

对于 $a\in G$，我们有：$b\in[a]_R$ 当且仅当 $\langle a, b\rangle\in R$，即当且仅当 $a^{-1}*b\in H$，而 $a^{-1}*b\in H$ 就是 $b\in aH$。因此，$[a]_R=aH$。

(b) 由于 R 是 G 中的一个等价关系，所以必定将 G 划分成不同的等价类 $[a_1]_R, [a_2]_R, \cdots, [a_k]_R$，使得

$$G=\bigcup_{i=1}^{k}[a_i]_R=\bigcup_{i=1}^{k}a_i H$$

又因，H 中任意两个不同的元素 h_1，h_2，$a\in G$，必有 $a*h_1\neq a*h_2$，所以 $|a_iH|=|H|=m$，$i=1, 2, \cdots, k$。因此

$$n=|G|=\left|\bigcup_{i=1}^{k}a_i H\right|=\sum_{i=1}^{k}|a_iH|=mk \qquad \square$$

根据拉格朗日定理，可直接得到以下几个推论。

推论 1 任何质数阶的群不可能有非平凡子群。

这是因为，如果有非平凡子群，那么该子群的阶必定是原来群的阶的一个因子，这就与原来群的阶是质数相矛盾。 □

推论 2 设 $\langle G, *\rangle$ 是 n 阶有限群，那么对于任意的 $a\in G$，a 的阶必是 n 的因子且必有 $a^n=e$，这里 e 是群 $\langle G, *\rangle$ 中的幺元。如果 n 为质数，则 $\langle G, *\rangle$ 必是循环群。

这是因为，由 G 中的任意元素 a 生成的循环群

$$H=\{a^i \mid i\in I, a\in G\}$$

一定是 G 的一个子群。如果 H 的阶是 m，那么由定理 5-5.3 可知 $a^m=e$，即 a 的阶等于 m。由拉格朗日定理必有 $n=mk$，$k\in N$，因此，a 的阶 m 是 n 的因子，且有

$$a^n=a^{mk}=(a^m)^k=e^k=e$$

因为质数阶群只有平凡子群，所以，质数阶群必定是循环群。必须注意，群的阶与元素的阶这两个概念的不同。 □

例题 1 设 $K=\{e, a, b, c\}$，在 K 上定义二元运算 $*$ 如表 5-7.1 所示。

表 5-7.1

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证明 $\langle K, *\rangle$ 是一个群，但不是循环群。

证明 由表 5-7.1 可知，运算 $*$ 是封闭的和可结合的。幺元是 e，每个元

素的逆元是自身，所以，$\langle K, *\rangle$ 是群。因为 a, b, c 都是二阶元，故 $\langle K, *\rangle$ 不是循环群。我们称 $\langle K, *\rangle$ 为Klein四元群。

例如，$S=\{1, 2, 3, 4\}$，置换群

$$\left\langle\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}, \circ\right\rangle$$

就是一个Klein四元群。

例题2 任何一个四阶群只可能是四阶循环群或者Klein四元群。

证明 设四阶群为 $\langle\{e, a, b, c\}, *\rangle$。其中 e 是幺元。当四阶群含有一个四阶元素时，这个群就是循环群。

当四阶群不含有四阶元素时，则由推论2可知，除幺元 e 外，a, b, c 的阶一定都是2。$a*b$ 不可能等于 a, b 或 e，否则将导致 $b=e$, $a=e$ 或 $a=b$ 的矛盾，所以 $a*b=c$。同样地有 $b*a=c$ 以及 $a*c=c*a=b$, $b*c=c*b=a$。因此，这个群是Klein四元群。

5-7 习题

(1) 设 $G=\{\varphi|\varphi: x\to ax+b$ 其中 $a, b\in R$ 且 $a\neq 0, x\in R\}$ 二元运算 $\circ$ 是映射的复合。

a) 证明 $\langle G, \circ\rangle$ 是一个群。

b) 若 S 和 T 分别是由 G 中 $a=1$ 和 $b=0$ 的所有映射构成的集合，证明 $\langle S, \circ\rangle$ 和 $\langle T, \circ\rangle$ 都是子群。

c) 写出 S 和 T 在 G 中所有的左陪集。

(2) 设 $\langle Z_6, +_6\rangle$ 是一个群，这里 $+_6$ 是模6加法，$Z_6=\{[0], [1], [2], [3], [4], [5]\}$，试写出 $\langle Z_6, +_6\rangle$ 中每个子群及其相应的左陪集。

(3) 设 $\langle G, *\rangle$ 是任一群，定义 $R\subseteq G\times G$ 为

$$R=\{\langle\sigma, \varphi\rangle \mid \text{存在 } \theta\in G \text{ 使得 } \varphi=\theta*\sigma*\theta^{-1}\}$$

验证 R 是 G 上的等价关系。

(4) 设 S_n 是一个对称群，G 是保持某一个元素不变的置换群，求出 G 在 S_n 中的所有左陪集。

(5) 设 $\langle H, *\rangle$ 是群 $\langle G, *\rangle$ 的子群，如果

$$A=\{x|x\in G, x*H*x^{-1}=H\}$$

证明 $\langle A, *\rangle$ 是 $\langle G, *\rangle$ 的一个子群。

(6) 证明，在由群 $\langle G, *\rangle$ 的一个子群 $\langle S, *\rangle$ 所确定的陪集中，只有一个陪集是子群。

(7) 设 aH 和 bH 是 H 在 G 中的两个左陪集，证明：要末 $aH \cap bH = \phi$，要末 $aH = bH$。

(8) 设 p 是质数，证明：p^m 阶群中一定包含着一个 p 阶子群。

(9) 设 $\langle S, *\rangle$ 和 $\langle T, *\rangle$ 分别是群 $\langle G, *\rangle$ 的 s 阶和 t 阶子群，并且 $S \cap T$ 和 $S \cup T$ 的阶分别为 μ 和 ν，证明 $st \geqslant \mu\nu$。

5-8 同态与同构

这一节，我们将讨论两个代数系统之间的联系。着重研究两个代数系统之间的同态关系和同构关系。

定义 5-8.1 设 $\langle A, \bigstar\rangle$ 和 $\langle B, *\rangle$ 是两个代数系统，$\bigstar$ 和 $*$ 分别是 A 和 B 上的二元(n 元)运算，设 f 是从 A 到 B 的一个映射，使得对任意的 $a_1, a_2 \in A$，有

$$f(a_1 \bigstar a_2) = f(a_1) * f(a_2)$$

则称 f 为由 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的一个同态映射，称 $\langle A, \bigstar\rangle$ 同态于 $\langle B, *\rangle$，记作 $A \sim B$。把 $\langle f(A), *\rangle$ 称为 $\langle A, \bigstar\rangle$ 的一个同态象。其中

$$f(A) = \{x \mid x = f(a),\ a \in A\} \subseteq B$$

两个代数系统在同态意义下的相互联系可以由图 5-8.1 来描述。

例 1 考察代数系统 $\langle I, \cdot\rangle$，这里 I 是整数集，$\cdot$ 是普通乘法运算。如果我们对运算结果只感兴趣于正、负、零之间的特征区别，那么，代数系统 $\langle I, \cdot\rangle$ 中运算结果的特征就可以用另一个代数系统 $\langle B, \odot\rangle$ 的运算结果来描述，其中 $B = \{正, 负, 零\}$，$\odot$ 是定义在 B 上的二元运算，如表 5-8.1 所示。

作映射 f: $I \to B$ 如下：

$$f(n) = \begin{cases} 正 & 若\ n > 0 \\ 负 & 若\ n < 0 \\ 零 & 若\ n = 0 \end{cases}$$

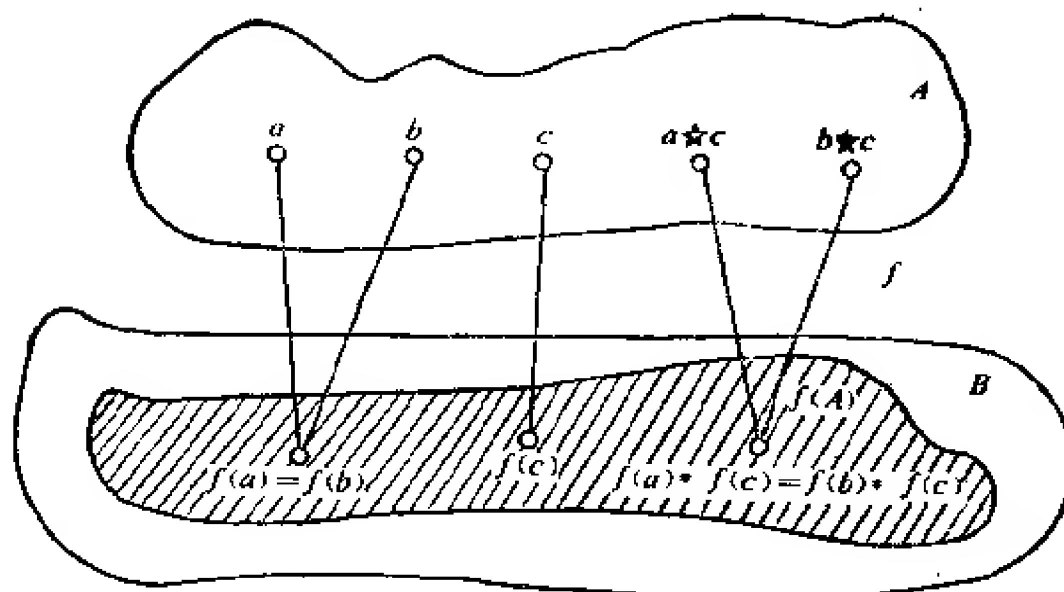


图 5-8.1

表 5-8.1

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

很明显，对于任意的 $a,\ b\in I$，有

$$f(a\cdot b)=f(a)\odot f(b)$$

因此，映射 f 是由 $\langle I,\ \cdot\rangle$ 到 $\langle B,\ \odot\rangle$ 的一个同态。

例 1 告诉我们，在 $\langle I,\ \cdot\rangle$ 中研究运算结果的正、负、零的特征就等于在 $\langle B,\ \odot\rangle$ 中的运算特征，可以说，代数系统 $\langle B,\ \odot\rangle$ 描述了 $\langle I,\ \cdot\rangle$ 中运算结果的这些基本特征。而这正是研究两个代数系统之间是否存在同态的重要意义。

应该指出，由一个代数系统到另一个代数系统可能存在着多于一个的同态。

定义 5-8.2 设 f 是由 $\langle A,\ \bigstar\rangle$ 到 $\langle B,\ *\rangle$ 的一个同态，如果 f 是从 A 到 B 的一个满射，则 f 称为满同态；如果 f 是从 A 到 B 的一个入射，则 f 称为单一同态；如果 f 是从 A 到 B 的一个双射，则 f 称为同构映射，并称 $\langle A,\ \bigstar\rangle$ 和 $\langle B,\ *\rangle$ 是同构的，记作 $A\cong B$。

例 2　设 $f: R \to R$ 定义为对任意 $x \in R$

$$f(x)=5^x$$

那么，f 是从 $\langle R, +\rangle$ 到 $\langle R, \cdot\rangle$ 的一个单一同态。

例 3　设 $f: N \to N_k$ 定义为对任意的 $x \in N$

$$f(x)=x \bmod k$$

那么，f 是从 $\langle N, +\rangle$ 到 $\langle N_k, +_k\rangle$ 的一个满同态。

例 4　设 $H=\{x \mid x=dn, d$ 是某一个正整数, $n \in I\}$，定义映射 $f: I \to H$ 为对任意 $n \in I$

$$f(n)=dn$$

那么，f 是 $\langle I, +\rangle$ 到 $\langle H, +\rangle$ 的一个同构。所以 $I \cong H$。

例题 1　设 $A=\{a, b, c, d\}$，在 A 上定义一个二元运算如表 5-8.2 所示。又设 $B=\{\alpha, \beta, \gamma, \delta\}$，在 B 上定义一个二元运算如表 5-8.3 所示。证明 $\langle A, \bigstar\rangle$ 和 $\langle B, *\rangle$ 是同构的。

表　5-8.2

★	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

表　5-8.3

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	α	γ
γ	β	δ	δ	γ
δ	α	β	γ	δ

证明　考察映射 f，使得

$$f(a)=\alpha \qquad f(b)=\beta$$
$$f(c)=\gamma \qquad f(d)=\delta$$

显然，f 是一个从 A 到 B 的双射，由表 5-8.2 和表 5-8.3 容易验证 f 是由 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的一个同态。因此，$\langle A, \bigstar\rangle$ 和 $\langle B, *\rangle$ 是同构的。

如果考察映射 g，使得

$$g(a)=\delta \qquad g(b)=\gamma$$
$$g(c)=\beta \qquad g(d)=\alpha$$

那么，g 也是由 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的一个同构。

例题 1 告诉我们，当两个代数系统是同构的话，它们之间的同构映射可以是不唯一的。

例 5　表 5-8.4 中的代数系统 $\langle B, \oplus\rangle$，和 $\langle C, *\rangle$ 都是与代数系统 $\langle A, \bigstar\rangle$ 同构的。

表　5-8.4

$\bigstar$	a	b
a	a	b
b	b	a

$\langle A, \bigstar\rangle$

$\oplus$	偶	奇
偶	偶	奇
奇	奇	偶

$\langle B, \oplus\rangle$

$*$	$0°$	$180°$
$0°$	$0°$	$180°$
$180°$	$180°$	$0°$

$\langle C, *\rangle$

同构这个概念很重要。从上例中可以看到，形式上不同的代数系统，如果它们是同构的话，那么，就可抽象地把它们看作是本质上相同的代数系统，所不同的只是所用的符号不同。并且，容易看出同构的逆仍是一个同构。

定义 5-8.3　设 $\langle A, \bigstar\rangle$ 是一个代数系统，如果 f 是由 $\langle A, \bigstar\rangle$ 到 $\langle A, \bigstar\rangle$ 的同态，则称 f 为自同态。如果 g 是由 $\langle A, \bigstar\rangle$ 到 $\langle A, \bigstar\rangle$ 的同构，则称 g 为自同构。

定理 5-8.1　设 G 是代数系统的集合，则 G 中代数系统之间

的同构关系是等价关系。

证明 因为任何一个代数系统 $\langle A, \bigstar\rangle$ 可以通过恒等映射与它自身同构，即自反性成立。关于对称性，设 $\langle A, \bigstar\rangle \cong \langle B, *\rangle$ 且有对应的同构映射 f，因为 f 的逆是由 $\langle B, *\rangle$ 到 $\langle A, \bigstar\rangle$ 的同构映射，即 $\langle B, *\rangle \cong \langle A, \bigstar\rangle$。最后，如果 f 是由 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的同构映射，g 是由 $\langle B, *\rangle$ 到 $\langle C, \triangle\rangle$ 的同构映射，那么 $g\circ f$ 就是 $\langle A, \bigstar\rangle$ 到 $\langle C, \triangle\rangle$ 的同构映射。因此，同构关系是等价关系。 □

定理 5-8.2 设 f 是从代数系统 $\langle A, \bigstar\rangle$ 到代数系统 $\langle B, *\rangle$ 的同态映射。

(a) 如果 $\langle A, \bigstar\rangle$ 是半群，那么在 f 作用下，同态象 $\langle f(A), *\rangle$ 也是半群。

(b) 如果 $\langle A, \bigstar\rangle$ 是独异点，那么在 f 作用下，同态象 $\langle f(A), *\rangle$ 也是独异点。

(c) 如果 $\langle A, \bigstar\rangle$ 是群，那么在 f 作用下，同态象 $\langle f(A), *\rangle$ 也是群。

证明 (a) 设 $\langle A, \bigstar\rangle$ 是半群且 $\langle B, *\rangle$ 是一个代数系统，如果 f 是由 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的一个同态映射，则 $f(A)\subseteq B$。

对于任意的 $a, b\in f(A)$，必有 $x, y\in A$ 使得

$$f(x)=a,\quad f(y)=b$$

在 A 中，必有 $z=x\bigstar y$，所以

$$a*b=f(x)*f(y)=f(x\bigstar y)=f(z)\in f(A)$$

最后，$*$ 在 $f(A)$ 上是可结合的，这是因为：对于任意的 $a, b, c\in f(A)$，必有 $x, y, z\in A$，使得

$$f(x)=a,\quad f(y)=b,\quad f(z)=c$$

因为 $\bigstar$ 在 A 上是可结合的，所以

$$\begin{aligned}a*(b*c)&=f(x)*(f(y)*f(z))=f(x)*f(y\bigstar z)\\&=f(x\bigstar(y\bigstar z))=f((x\bigstar y)\bigstar z)\\&=f(x\bigstar y)*f(z)=(f(x)*f(y))*f(z)\\&=(a*b)*c\end{aligned}$$

因此，$\langle f(A), *\rangle$ 是半群。

(b) 设 $\langle A, \bigstar\rangle$ 是独异点，e 是 A 中的幺元，那么 $f(e)$ 是 $f(A)$ 中的幺元。这是因为对于任意的 $a\in f(A)$ 必有 $x\in A$ 使

$$f(x)=a$$

所以

$$\begin{aligned}a*f(e)&=f(x)*f(e)=f(x\bigstar e)=f(x)=a\\&=f(e\bigstar x)=f(e)*f(x)=f(e)*a\end{aligned}$$

因此，$\langle f(A), *\rangle$ 是独异点。

(c) 设 $\langle A, \bigstar\rangle$ 是群。

对于任意的 $a\in f(A)$ 必有 $x\in A$ 使

$$f(x)=a$$

因为 $\langle A, \bigstar\rangle$ 是群，故 x 有逆元 x^{-1}，且 $f(x^{-1})\in f(A)$，而

$$\begin{aligned}f(x)*f(x^{-1})&=f(x\bigstar x^{-1})=f(e)=f(x^{-1}\bigstar x)\\&=f(x^{-1})*f(x)\end{aligned}$$

所以，$f(x^{-1})$ 是 $f(x)$ 的逆元。即

$$f(x^{-1})=f(x)^{-1}。$$

因此，$\langle f(A), *\rangle$ 是群。 □

定义 5-8.4 设 f 是由群 $\langle G, \bigstar\rangle$ 到群 $\langle G', *\rangle$ 的同态映射，e' 是 G' 中的幺元，记 $\mathrm{Ker}(f)=\{x|x\in G$ 且 $f(x)=e'\}$，称 $\mathrm{Ker}(f)$ 为同态映射 f 的核，简称 f 的同态核。

定理 5-8.3 设 f 是由群 $\langle G, \bigstar\rangle$ 到群 $\langle G', *\rangle$ 的同态映射，则 f 的同态核 K 是 G 的子群。

证明 由定理 5-8.2 可知，$e'=f(e)$。设 $k_1, k_2\in K$，则

$$f(k_1\bigstar k_2)=f(k_1)*f(k_2)=e'*e'=e'$$

故 $k_1\bigstar k_2\in K$。

对任意的 $k\in K$，由定理 5-8.2 可知

$$f(k^{-1})=f(k)^{-1}=e'^{-1}=e'$$

故 $k^{-1}\in K$。因此，$\langle K, \bigstar\rangle$ 是 $\langle G, \bigstar\rangle$ 的子群。 □

下面，我们进一步讨论同态与同余关系的对应。为此先介绍同余关系的概念。

定义 5-8.5 设 $\langle A, ★\rangle$ 是一个代数系统，并设 R 是 A 上的一个等价关系。如果当 $\langle a_1, a_2\rangle, \langle b_1, b_2\rangle \in R$ 时，蕴涵着 $\langle a_1★b_1, a_2★b_2\rangle \in R$，则称 R 为 A 上关于 ★ 的同余关系。由这个同余关系将 A 划分成的等价类就称为同余类。

例 6 设 $A=\{a, b, c, d\}$，对于由表 5-8.5 所确定的代数系统 $\langle A, ★\rangle$ 以及由表 5-8.6 所定义的在 A 上的等价关系 R。容易

表 5-8.5

★	a	b	c	d
a	a	a	d	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	a

$\langle A, ★\rangle$

表 5-8.6

	a	b	c	d
a	✓	✓		
b	✓	✓		
c			✓	✓
d			✓	✓

R

验证，R 是 A 上的同余关系。这个同余关系将 A 划分成同余类为 $\{a, b\}$ 和 $\{c, d\}$。

例 7 设 $A=\{a, b, c, d\}$，对于由表 5-8.7 所确定的代数系统 $\langle A, ★\rangle$ 以及由表 5-8.6 所定义的在 A 上的等价关系 R。

表 5-8.7

★	a	b	c	d
a	a	a	d	c
b	b	a	d	a
c	c	b	a	b
d	c	d	b	a

$\langle A, ★\rangle$

由于对 $\langle a, b\rangle, \langle c, d\rangle \in R$ 有

$$\langle a★c,\ b★d\rangle = \langle d,\ a\rangle \notin R$$

因此，由表 5-8.6 所定义的在 A 上的等价关系 R 不是一个同余关系。

由上述两例可知：在 A 上定义的等价关系 R，不一定是 A 上的同余关系，这是因为同余关系必须与定义在 A 上的二元运算密切相关。

定理 5-8.4 设 $\langle A, ★\rangle$ 是一个代数系统，R 是 A 上的一个同余关系，$B=\{A_1, A_2, \cdots, A_r\}$ 是由 R 诱导的 A 的一个划分，那么，必定存在新的代数系统 $\langle B, *\rangle$，它是 $\langle A, ★\rangle$ 的同态象。

证明 在 B 上定义二元运算 $*$ 为：对于任意的 $A_i, A_j \in B$，任取 $a_1 \in A_i$，$a_2 \in A_j$，如果 $a_1★a_2 \in A_k$，则 $A_i * A_j = A_k$。由于 R 是 A 上的同余关系，所以，以上定义的 $A_i * A_j = A_k$ 是唯一的。

作映射 $\quad f(a) = A_i \quad a \in A_i$

显然，f 是从 A 到 B 的满映射。

对于任意的 $x, y \in A$，x, y 必属于 B 中的某两个同余类，不妨设 $x \in A_i$，$y \in A_j$，$1 \leqslant i, j \leqslant r$；同时，$x★y$ 必属于 B 中某个同余类，不妨设 $x★y \in A_k$，于是，就有

$$f(x★y) = A_k = A_i * A_j = f(x) * f(y)$$

因此，f 是由 $\langle A, ★\rangle$ 到 $\langle R, *\rangle$ 的满同态，即 $\langle B, *\rangle$ 是 $\langle A, ★\rangle$ 的同态象。 □

定理 5-8.5 设 f 是由 $\langle A, ★\rangle$ 到 $\langle B, *\rangle$ 的一个同态映射，如果在 A 上定义二元关系 R 为：$\langle a, b\rangle \in R$ 当且仅当

$$f(a) = f(b)$$

那么，R 是 A 上的一个同余关系。

证明 因为 $f(a) = f(a)$，所以 $\langle a, a\rangle \in R$。若 $\langle a, b\rangle \in R$，则 $f(a) = f(b)$ 即 $f(b) = f(a)$，所以 $\langle b, a\rangle \in R$。若 $\langle a, b\rangle \in R$，$\langle b, c\rangle \in R$ 则 $f(a) = f(b) = f(c)$，所以 $\langle a, c\rangle \in R$。
最后，又因为若 $\langle a, b\rangle \in R$，$\langle c, d\rangle \in R$，则有

$$f(a★c) = f(a) * f(c) = f(b) * f(d) = f(b★d)$$

所以，$\langle a\bigstar c, b\bigstar d\rangle \in R$。

因此，R 是 A 上的同余关系。 □

形象地说，一个代数系统的同态象可以看作是当抽去该系统中某些元素的次要特性的情况下，对该系统的一种粗糙描述。如果我们把属于同一个同余类的元素看作是没有区别的，那么原系统的性态可以用同余类之间的相互关系来描述。现在，用一个例子来说明这一点。

例 8 如表 5-8.8 所确定的两个代数系统 $\langle A, \bigstar\rangle$ 和 $\langle B, *\rangle$。

表 5-8.8

	α	β	γ	δ	ε	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	ε
γ	α	γ	α	β	γ	ε
δ	α	β	β	δ	ε	ζ
ε	γ	γ	γ	ε	ε	ζ
ζ	δ	ε	ε	ζ	ζ	ζ

$\langle A, \bigstar\rangle$

*	1	0	−1
1	1	1	0
0	1	0	−1
−1	0	−1	−1

$\langle B, *\rangle$

映射
$$f(\alpha)=1 \quad f(\beta)=1 \quad f(\gamma)=1$$
$$f(\delta)=0 \quad f(\varepsilon)=0 \quad f(\zeta)=-1$$
明显地是由代数系统 $\langle A, \bigstar\rangle$ 到 $\langle B, *\rangle$ 的一个同态映射。假如把代数系统 $\langle A, \bigstar\rangle$ 看作是对六个带电粒子 $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ 相互作用的详尽描述。如果 α, β, γ 是带正电荷的粒子；δ, ε 是中性粒子；ζ 是带负电荷的粒子，那么，我们就可用 1, 0, −1 分别表示这三类粒子，这就是映射 f 所具有的特性。若记
$$B=\{1, 0, -1\}$$

那么，代数系统 $\langle B, *\rangle$ 描述了这三类粒子的相互作用，它正好是代数系统 $\langle A, ★\rangle$ 的粗糙描述。

5-8 习题

(1) 证明：如果 f 是由 $\langle A, ★\rangle$ 到 $\langle B, *\rangle$ 的同态映射，g 是由 $\langle B, *\rangle$ 到 $\langle C, \triangle\rangle$ 的同态映射，那么，$g\circ f$ 是由 $\langle A, ★\rangle$ 到 $\langle C, \triangle\rangle$ 的同态映射。

(2) 设 $\langle G, *\rangle$ 是一个群，而 $a\in G$，如果 f 是从 G 到 G 的映射，使得对于每一个 $x\in G$，都有

$$f(x)=a*x*a^{-1}$$

试证明 f 是一个从 G 到 G 上的自同构。

(3) 试证由表 5-8.9 所给出的两个群 $\langle G, ★\rangle$ 和 $\langle S, *\rangle$ 是同构的。

表 5-8.9

★	p_1	p_2	p_3	p_4
p_1	p_1	p_2	p_3	p_4
p_2	p_2	p_1	p_4	p_3
p_3	p_3	p_4	p_1	p_2
p_4	p_4	p_3	p_2	p_1

$\langle G, ★\rangle$

*	q_1	q_2	q_3	q_4
q_1	q_3	q_4	q_1	q_2
q_2	q_4	q_3	q_2	q_1
q_3	q_1	q_2	q_3	q_4
q_4	q_2	q_1	q_4	q_3

$\langle S, *\rangle$

(4) 设 f_1, f_2 都是从代数系统 $\langle A, ★\rangle$ 到代数系统 $\langle B, *\rangle$ 的同态。设 g 是从 A 到 B 的一个映射，使得对任意 $a\in A$，都有

$$g(a)=f_1(a)*f_2(a)$$

证明：如果 $\langle B, *\rangle$ 是一个可交换半群，那么 g 是一个由 $\langle A, ★\rangle$ 到 $\langle B, *\rangle$ 的同态。

(5) $\langle R, +\rangle$ 是实数集上的加法群，设

$$f: x\to e^{2\pi ix},\ x\in R$$

f 是同态否？如果是，请写出同态象和同态核。

(6) 证明：循环群的同态象必定是循环群。

(7) $\langle R-\{0\}, \times\rangle$ 与 $\langle R, +\rangle$同构吗？

(8) 证明：一个集合上任意两个同余关系的交也是一个同余关系。

(9) 证明定理5-8.4中在B上所定义的二元运算 $*$ 是唯一确定的。

(10) 考察代数系统 $\langle I, +\rangle$，以下定义在 I 上的二元关系 R 是同余关系吗？

a) $\langle x, y\rangle \in R$ 当且仅当 $(x<0 \wedge y<0) \vee (x\geqslant 0 \wedge y\geqslant 0)$

b) $\langle x, y\rangle \in R$ 当且仅当 $|x-y|<10$

c) $\langle x, y\rangle \in R$ 当且仅当 $(x=y=0) \vee (x\neq 0 \wedge y\neq 0)$

d) $\langle x, y\rangle \in R$ 当且仅当 $x\geqslant y$

(11) 设 f 和 g 都是群 $\langle G_1, \bigstar\rangle$ 到群 $\langle G_2, *\rangle$ 的同态，证明 $\langle C, \bigstar\rangle$ 是 $\langle G_1, \bigstar\rangle$ 的一个子群，其中

$$C=\{x|x\in G_1 \text{且} f(x)=g(x)\}$$

(12) 设 f 为从群 $\langle G_1, *\rangle$ 到 $\langle G_2, \triangle\rangle$ 的同态映射，则 f 为入射当且仅当 $\mathrm{Ker}(f)=\{e\}$。其中，e 是 G_1 中的幺元。

5-9 环 与 域

以上，我们已初步研究了具有一个二元运算的代数系统——半群、独异点、群。接着，我们将讨论具有两个二元运算的代数系统。对于给定的两个代数系统 $\langle A, \bigstar\rangle$ 和 $\langle A, *\rangle$，容易将它们组合成一个具有两个二元运算的代数系统 $\langle A, \bigstar, *\rangle$。我们感兴趣于两个二元运算 $\bigstar$ 和 $*$ 之间有联系的代数系统 $\langle A, \bigstar, *\rangle$，通常，我们把第一个二元运算 $\bigstar$ 称为“加法”，把第二个运算 $*$ 称为“乘法”。

例如，具有加法和乘法这两个二元运算的实数系统 $\langle R, +, \times\rangle$和整数系统 $\langle I, +, \times\rangle$ 都是我们很熟悉的代数系统。对于任意的 $a, b, c\in R$ (或 I)，都有 $a\times(b+c)=(a\times b)+(a\times c)$以及$(b+c)\times a=(b\times a)+(c\times a)$，这种联系就是乘法运算对于加法运算是可分配的。

定义 5-9.1 设 $\langle A, \bigstar, *\rangle$ 是一个代数系统，如果满足：

(1) $\langle A, \bigstar\rangle$ 是阿贝尔群。

(2) $\langle A, *\rangle$ 是半群。

(3) 运算 $*$ 对于运算★是可分配的。

则称 $\langle A, ★, *\rangle$ 是环。

根据定义可以清楚地看到，整数集合、有理数集合、偶数集合、复数集合以及定义在这些集合上的普通加法和乘法运算都是可构成环的例子。

例 1 系数属于实数的所有 x 的多项式所组成的集合记作 $R[x]$，那么，$R[x]$ 关于多项式的加法和乘法构成一个环。

例 2 元素属于实数的所有 n 阶矩阵所组成的集合记作 $(R)_n$，那么，$(R)_n$ 关于矩阵的加法和乘法构成一个环。

例题 1 设 $\langle K, *\rangle$ 是 Klein 四元群，其中 $K=\{e, a, b, c\}$，$*$ 的运算见表 5-7.1。如果再定义 K 上的二元运算 $\cdot$ 如表 5-9.1 所示。

表 5-9.1

$\cdot$	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

则 $\langle K, *, \cdot\rangle$ 是一个环。

证明 先证 $\langle K, \cdot\rangle$ 是半群。

由表 5-9.1 可知，对于任意的 $x\in K$ 都有 $x\cdot e=e\cdot x=e$; a 和 c 都是关于运算 $\cdot$ 的右幺元；对于任意的 $x\in K$ 都有 $x\cdot b=e$。

对于任意的 $x, y, z\in K$，可以证明必有 $(x\cdot y)\cdot z=x\cdot(y\cdot z)$，这是因为：

如果 $z=e$ 或 $z=b$，那么，$(x\cdot y)\cdot z=e=x\cdot(y\cdot z)$

如果 $z=a$ 或 $z=c$，那么，$(x\cdot y)\cdot z=x\cdot y=x\cdot(y\cdot z)$

其次证明 $\cdot$ 关于 $*$ 是可分配的。

先证等式 $(y*z)\cdot x=(y\cdot x)*(z\cdot x)$

如果 $x=e$ 或 $x=b$，那么，$(y*z)\cdot x=e=e*e=(y\cdot x)*(z\cdot x)$

如果 $x=a$ 或 $x=c$，那么，$(y*z)\cdot x=(y\cdot x)*(z\cdot x)$

再证等式 $x\cdot(y*z)=(x\cdot y)*(x\cdot z)$

如果 $y=z$ 则 $y*z=e$，所以

$$x\cdot(y*z)=x\cdot e=e$$

$$(x\cdot y)*(x\cdot z)=(x\cdot y)*(x\cdot y)=e$$

如果 y 与 z 中有一个等于 e，则等式 $x\cdot(y*z)=(x\cdot y)*(x\cdot z)$ 成立。

如果 y, z 均不等于 e，且 $y\neq z$，那么有以下三种情况：

(1) $x\cdot(a*b)=x$ 且 $(x\cdot a)*(x\cdot b)=x*e=x$

(2) $x\cdot(a*c)=x\cdot b=e$ 且 $(x\cdot a)*(x\cdot c)=x*x=e$

(3) $x\cdot(b*c)=x\cdot a=x$ 且 $(x\cdot b)*(x\cdot c)=e*x=x$

所以，在代数系统 $\langle K, *, \cdot\rangle$ 中运算 $\cdot$ 对于运算 $*$ 是可分配的。因此，$\langle K, *, \cdot\rangle$ 是一个环。

定理5-9.1 设 $\langle A, +, \cdot\rangle$ 是一个环，则对任意的 $a, b, c\in A$，有

(1) $a\cdot\theta=\theta\cdot a=\theta$

(2) $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$

(3) $(-a)\cdot(-b)=a\cdot b$

(4) $a\cdot(b-c)=a\cdot b-a\cdot c$

(5) $(b-c)\cdot a=b\cdot a-c\cdot a$

其中，θ 是加法幺元，$-a$ 是 a 的加法逆元，并将 $a+(-b)$ 记为 $a-b$。

证明 (1) 因为

$$\theta\cdot a=(\theta+\theta)\cdot a=\theta\cdot a+\theta\cdot a$$

由消去律，即得

$$\theta\cdot a=\theta$$

同理可证 $a\cdot\theta=\theta$

(2) 因为

$$a\cdot b+a\cdot(-b)=a\cdot[b+(-b)]=a\cdot\theta=\theta$$

所以 $a\cdot(-b)=-(a\cdot b)$

同理可证 $(-a)\cdot b=-(a\cdot b)$

(3) 因为

$$a\cdot(-b)+(-a)\cdot(-b)=[a+(-a)]\cdot(-b)$$
$$=\theta\cdot(-b)=\theta$$

和 $a\cdot(-b)+a\cdot b=a\cdot[(-b)+b]=a\cdot\theta=\theta$

所以 $(-a)\cdot(-b)=a\cdot b$

(4) $a\cdot(b-c)=a\cdot[b+(-c)]=a\cdot b+a\cdot(-c)$

$=a\cdot b+(-a\cdot c)=a\cdot b-a\cdot c$

(5) $(b-c)\cdot a=[b+(-c)]\cdot a=b\cdot a+(-c)\cdot a$

$=b\cdot a+(-c\cdot a)=b\cdot a-c\cdot a$ □

我们还可以根据 $\langle A,\ \cdot\rangle$ 的结构来定义一些常见的特殊环。

定义 5-9.2 设 $\langle A,\ +,\ \cdot\rangle$ 是环。如果 $\langle A,\ \cdot\rangle$ 是可交换的，则称 $\langle A,\ +,\ \cdot\rangle$ 是交换环。如果 $\langle A,\ \cdot\rangle$ 含有幺元，则称 $\langle A,\ +,\ \cdot\rangle$ 是含幺环。

例 3 设 S 是一个集合，$\mathscr{P}(S)$ 是它的幂集，如果在 $\mathscr{P}(S)$ 上定义二元运算 + 和 · 如下：对于任意的 $A,\ B\in\mathscr{P}(S)$

$$A+B=\{x \mid (x\in S)\wedge(x\in A\vee x\in B)\wedge(x\notin A\cap B)\}$$

$$A\cdot B=A\cap B$$

容易证明 $\langle\mathscr{P}(S),\ +,\ \cdot\rangle$ 是一个环，称它为 S 的子集环。

由于集合运算 ∩ 是可交换的，且 $\langle\mathscr{P}(S),\ \cdot\rangle$ 含有幺元 S，因此子集环是含幺交换环。

定义 5-9.3 设 $\langle A,\ +,\ \cdot\rangle$ 是一个代数系统，如果满足：

1．$\langle A,\ +\rangle$ 是阿贝尔群。

2．$\langle A,\ \cdot\rangle$ 是可交换独异点，且无零因子，即对任意的 $a,\ b\in A$，$a\neq\theta$，$b\neq\theta$ 必有 $a\cdot b\neq\theta$。

3．运算 · 对于运算 + 是可分配的。

则称 $\langle A,\ +,\ \cdot\rangle$ 是整环。

例 4 因为 $\langle I,\ +\rangle$ 是一个具有加法幺元 0，且对任意 n 有逆元 $-n$ 的阿贝尔群；$\langle I,\ \cdot\rangle$ 是可交换独异点，且满足无零因子条件；运算 · 对于运算 + 是可分配的，故 $\langle I,\ +,\ \cdot\rangle$ 是整环。

定理 5-9.2 在整环 $\langle A,\ +,\ \cdot\rangle$ 中的无零因子条件等价于乘法消去律，即对于 $c\neq\theta$ 和 $c\cdot a=c\cdot b$，必有 $a=b$。

证明 若无零因子并设 $c\neq\theta$ 和 $c\cdot a=c\cdot b$，则有

$$c\cdot a-c\cdot b=c\cdot(a-b)=\theta$$

所以，必有 $a=b$。

反之，若消去律成立，设 $a\neq\theta$，$a\cdot b=\theta$ 则 $a\cdot b=a\cdot\theta$ 消去 a 即得 $b=\theta$。 □

定义 5-9.4 设 $\langle A, +, \cdot\rangle$ 是一个代数系统，如果满足：

1. $\langle A, +\rangle$ 是阿贝尔群。
2. $\langle A-\{\theta\}, \cdot\rangle$ 是阿贝尔群。
3. 运算 · 对于运算 + 是可分配的。

则称 $\langle A, +, \cdot\rangle$ 是域。

例如，$\langle Q, +, \cdot\rangle$，$\langle R, +, \cdot\rangle$，$\langle C, +, \cdot\rangle$ 都是域，这里，Q 为有理数集合，R 是实数集合，C 是复数集合，而 +，· 分别是各数集上的加法和乘法运算。

必须指出，$\langle I, +, \cdot\rangle$ 是整环，但不是域，因为 $\langle I-\{0\}, \cdot\rangle$ 不是群。这说明，整环不一定是域。

定理 5-9.3 域一定是整环。

证明 设 $\langle A, +, \cdot\rangle$ 是任一域。对于 $a, b, c\in A$ 且 $a\neq\theta$，如果有 $a\cdot b=a\cdot c$，(而 1 是乘法幺元)则

$$b=1\cdot b=(a^{-1}\cdot a)\cdot b=a^{-1}\cdot(a\cdot b)=a^{-1}\cdot(a\cdot c)$$
$$=(a^{-1}\cdot a)\cdot c=1\cdot c=c$$

因此，$\langle A, +, \cdot\rangle$ 是一个整环。 □

定理 5-9.4 有限整环必定是域。

证明 设 $\langle A, +, \cdot\rangle$ 是一个有限整环。

所以，对于 $a, b, c\in A$ 且 $c\neq\theta$，若 $a\neq b$ 则 $a\cdot c\neq b\cdot c$。再由运算 · 的封闭性，就有 $A\cdot c=A$。

对于乘法幺元 1，由 $A\cdot c=A$，必有 $d\in A$，使得 $d\cdot c=1$，故 d 是 c 的乘法逆元。

因此，有限整环 $\langle A, +, \cdot\rangle$ 是一个域。 □

接着，我们将讨论具有两个二元运算的代数系统之间的同态。

定义 5-9.5 设 $\langle A, +, \cdot\rangle$ 和 $\langle B, \triangle, \blacktriangle\rangle$ 是两个代数系统，如果一个从 A 到 B 的映射 f，满足如下条件：

对于任意的 $a, b\in A$，有

1. $f(a+b)=f(a)\overset{+}{\triangle}f(b)$

2. $f(a\cdot b)=f(a)\overset{\cdot}{\triangle}f(b)$

则称 f 为由 $\langle A, +, \cdot\rangle$ 到 $\langle B, \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$ 的一个同态映射，并称 $\langle f(A), \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$ 是 $\langle A, +, \cdot\rangle$ 的同态象。

类似于5-8节中所讨论，设 $\langle A, +, \cdot\rangle$ 是一个代数系统，并设 R 是一个在 A 上同时关于运算 $+$ 和 $\cdot$ 的同余关系，即 R 是 A 上的一个等价关系，并且，若 $\langle a_1, a_2\rangle$，$\langle b_1, b_2\rangle\in R$，则 $\langle a_1+b_1, a_2+b_2\rangle$，$\langle a_1\cdot b_1, a_2\cdot b_2\rangle\in R$。设 $B=\{A_1, A_2, \cdots, A_r\}$ 是由同余关系 R 诱导的 A 的划分，其中，$A_i(i=1, 2, \cdots, r)$ 都是同余类。我们在 B 上定义两个二元运算 $\overset{+}{\triangle}$ 和 $\overset{\cdot}{\triangle}$ 如下：

$$A_i\overset{+}{\triangle}A_j=A_k \qquad a_1+a_2\in A_k$$

$$A_i\overset{\cdot}{\triangle}A_j=A_l \qquad a_1\cdot a_2\in A_l$$

其中，$a_1\in A_i$，$a_2\in A_j$。

如果我们定义一个由 A 到 B 的映射 f：

对于 $a\in A$，使得

$$f(a)=A_i \qquad a\in A_i$$

那么，对于任意的 x，$y\in A$，必有 $x\in A_i$，$y\in A_j$ 以及

$$f(x+y)=A_k \qquad x+y\in A_k$$

而 $$A_k=A_i\overset{+}{\triangle}A_j=f(x)\overset{+}{\triangle}f(y)$$

所以 $$f(x+y)=f(x)\overset{+}{\triangle}f(y)$$

类似地可有 $$f(x\cdot y)=f(x)\overset{\cdot}{\triangle}f(y)$$

因此，f 是一个由 $\langle A, +, \cdot\rangle$ 到 $\langle B, \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$ 的同态映射，故 $\langle B, \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$ 是 $\langle A, +, \cdot\rangle$ 的一个同态象。

例5 设 $\langle N, +, \cdot\rangle$ 是一个代数系统，N 是自然数集，$+$ 和 $\cdot$ 是普通的加法和乘法运算，并设代数系统 $\langle\{偶, 奇\}, \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$，其运算表如表5-9.2所示。

容易验证映射

$$f(n)=\begin{cases}偶 & 若\ n=2k,\ k=0, 1, 2, \cdots\\ 奇 & 若\ n=2k+1,\ k=0, 1, 2, \cdots\end{cases}$$

是由 $\langle N, +, \cdot\rangle$ 到 $\langle\{偶, 奇\}, \overset{+}{\triangle}, \overset{\cdot}{\triangle}\rangle$ 的同态映射，因此，

表 5-9.2

$\triangle_{+}$	偶	奇
偶	偶	奇
奇	奇	偶

$\triangle_{\cdot}$	偶	奇
偶	偶	偶
奇	偶	奇

$\langle\{偶, 奇\}, \triangle_{+}, \triangle_{\cdot}\rangle$ 是 $\langle N, +, \cdot\rangle$ 的一个同态象。

定理5-9.5 任一环的同态象是一个环。

证明 设 $\langle A, +, \cdot\rangle$ 是一个环且 $\langle B, \triangle_{+}, \triangle_{\cdot}\rangle$ 是关于同态映射 f 的同态象。

由 $\langle A, +\rangle$ 是阿贝尔群，容易证明 $\langle B, \triangle_{+}\rangle$ 也是阿贝尔群。

由 $\langle A, \cdot\rangle$ 是半群容易证明 $\langle B, \triangle_{\cdot}\rangle$ 也是半群。

对于任意的 $b_1, b_2, b_3 \in B$，必有相应的 a_1, a_2, a_3，使得

$$f(a_i)=b_i \quad (i=1, 2, 3)$$

于是

$$\begin{aligned}
b_1 \triangle_{\cdot} (b_2 \triangle_{+} b_3) &= f(a_1) \triangle_{\cdot} (f(a_2) \triangle_{+} f(a_3)) \\
&= f(a_1) \triangle_{\cdot} f(a_2+a_3) \\
&= f(a_1 \cdot (a_2+a_3)) \\
&= f((a_1 \cdot a_2)+(a_1 \cdot a_3)) \\
&= f(a_1 \cdot a_2) \triangle_{+} f(a_1 \cdot a_3) \\
&= (f(a_1) \triangle_{\cdot} f(a_2)) \triangle_{+} (f(a_1) \triangle_{\cdot} f(a_3)) \\
&= (b_1 \triangle_{\cdot} b_2) \triangle_{+} (b_1 \triangle_{\cdot} b_3)
\end{aligned}$$

同理可证 $(b_2 \triangle_{+} b_3) \triangle_{\cdot} b_1 = (b_2 \triangle_{\cdot} b_1) \triangle_{+} (b_3 \triangle_{\cdot} b_1)$

因此，$\langle B, \triangle_{+}, \triangle_{\cdot}\rangle$ 也是一个环。 □

5-9 习题

(1) 已知一个环 $\langle\{a, b, c, d\}, +, \cdot\rangle$，它的运算由表 5-9.3 给出：

表 5-9.3

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

·	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	a

它是一个交换环吗？ 它有乘法幺元吗？ 这个环中的零元是什么？ 并求出每个元素的加法逆元。

(2) 试证 $\langle I, \triangle\!\!\!\!\cdot\,, \triangle \rangle$ 是有幺元的交换环，其中，运算 $\triangle\!\!\!\!\cdot$ 和 $\triangle$ 分别定义为：对任意的 $a, b \in I$, $a \triangle\!\!\!\!\cdot\, b = a + b - 1$, $a \triangle b = a + b - a \cdot b$。

(3) 设 $\langle R, +, \cdot \rangle$ 是一个环，证明：

如果 $a, b \in R$, 则 $(a+b)^2 = a^2 + a \cdot b + b \cdot a + b^2$。 其中，$x^2 = x \cdot x$。

(4) 设 $\langle A, +, \cdot \rangle$ 是一个代数系统，其中 $+$，$\cdot$ 为普通的加法和乘法运算，A 为下列集合：

a) $A = \{x \mid x = 2n, n \in I\}$

b) $A = \{x \mid x = 2n+1, n \in I\}$

c) $A = \{x \mid x \geqslant 0 \text{ 且 } x \in I\}$

d) $A = \{x \mid x = a + b\sqrt[4]{5}, a, b \in R\}$

e) $A = \{x \mid x = a + b\sqrt{3}, a, b \in R\}$

问 $\langle A, +, \cdot \rangle$ 是整环吗？ 为什么？

(5) 证明 $\langle \{0, 1\}, \oplus, \odot \rangle$ 是一个整环，其中运算 $\oplus$ 和 $\odot$ 由表 5-9.4 定义。

表 5-9.4

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

(6) 设 $\langle A, +, \cdot \rangle$ 是一个环，并且对于任意的 $a \in A$ 都有 $a \cdot a = a$，证明：

a) 对于任意的 $a \in A$，都有 $a + a = \theta$，其中 θ 是加法幺元。

b) $\langle A, +, \cdot \rangle$ 是可交换环。

(7) 设 $\langle A, +, \cdot \rangle$ 是一个代数系统，其中 $+$，$\cdot$ 为普通的加法和乘法运算，A 为下列集合：

a) $A = \{x \mid x \geqslant 0, x \in I\}$

b) $A = \{x \mid x = a + b\sqrt{3}, a, b \text{ 均为有理数}\}$

c) $A = \{x \mid x = a + b\sqrt[4]{5}, a, b \text{ 均为有理数}\}$

d) $A = \{x \mid x = a + b\sqrt{5}, a, b \text{ 均为有理数}\}$

e) $A = \{x \mid x = \frac{a}{b}, a, b \in I_+ \text{ 且 } a \neq k \cdot b\}$

问 $\langle A, +, \cdot \rangle$ 是域否？ 为什么？

(8) 设$\langle F, +, \cdot\rangle$是一个域，$S_1 \subseteq F$，$S_2 \subseteq F$，且$\langle S_1, +, \cdot\rangle$，$\langle S_2, +, \cdot\rangle$都构成域，证明$\langle S_1 \cap S_2, +, \cdot\rangle$也构成一个域。

*(9) 设$\langle A, \bigstar, *\rangle$是一个关于运算$\bigstar$和$*$分别具有幺元$e_1$和$e_2$的代数系统，并且运算$\bigstar$和$*$彼此之间是可分配的，证明对于$A$中所有的$x$，成立着$x \bigstar x = x * x = x$。

(10) 设$\langle A, \bigstar, *\rangle$是一个代数系统，且对于任意的$a \in A$，有

$$a \bigstar b = a$$

证明二元运算$*$对于$\bigstar$是可分配的。

第六章　格和布尔代数

这一章将介绍另一类代数系统，这就是格。格论大体上是在1935年左右形成的，它不仅是代数学的一个分支，而且在近代解析几何，半序空间等方面也都有重要的作用。我们在这里只介绍格的一些基本知识以及几个具有特别性质的格——分配格、有补格，在此基础上再介绍布尔代数，而布尔代数在计算机科学中有很多直接应用。

6-1　格的概念

在第三章中，我们介绍了偏序集的概念，偏序集就是由一个集合 A 以及 A 上的一个偏序关系"$\preccurlyeq$"所组成的一个代数系统 $\langle A, \preccurlyeq\rangle$。我们知道，对于偏序集来说，它的任一子集不是必定存在最小上界或最大下界的。例如，在由图 6-1.1 所示的偏序集中，$\{a, b\}$ 的最小上界是 c，但没有最大下界；$\{e, f\}$ 的最大下界是 d，但没有最小上界。

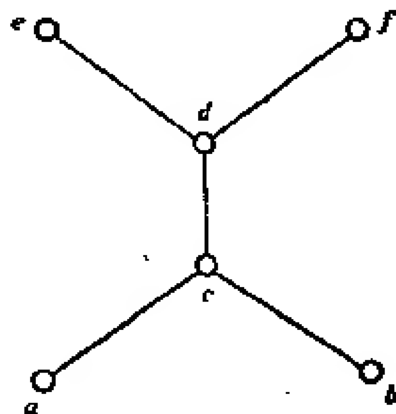


图　6-1.1

今后，我们把 $\{a, b\}$ 的最小上界（最大下界）称为元素 a，b 的最小上界（最大下界）。

然而，由图 6-1.2 所示的那些偏序集却都有这样一个共同的特性，那就是在这些偏序集中，任何两个元素都有最小上界和最大下界。我们把具有这种性质的偏序集称作格。

定义 6-1.1　设 $\langle A, \preccurlyeq\rangle$ 是一个偏序集，如果 A 中任意两个元素都有最小上界和最大下界，则称 $\langle A, \preccurlyeq\rangle$ 为格。

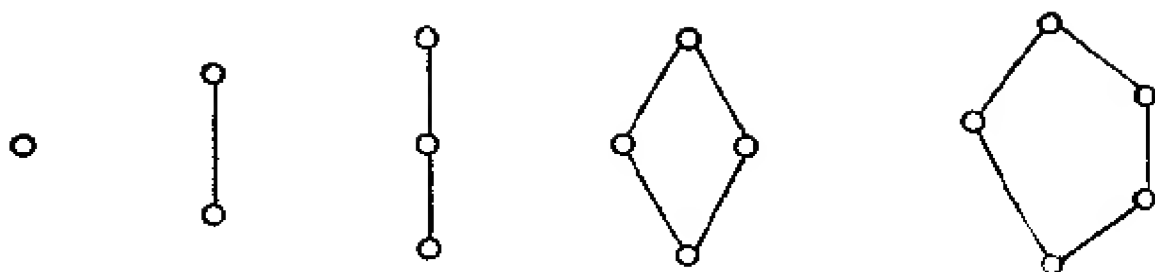


图 6-1.2

例 1 设 I_+ 是所有正整数的集合，在 I_+ 上定义一个二元关系 $|$，对于 $a, b \in I_+$，$a|b$ 当且仅当 a 整除 b。容易验证 $|$ 是 I_+ 上的一个偏序关系，故 $\langle I_+, |\rangle$ 是偏序集。由于该偏序集中任意两个元素的最小公倍数、最大公约数就是这两个元素的最小上界和最大下界，因此，$\langle I_+, |\rangle$ 是格。

例 2 设 $\mathscr{P}(S)$ 是给定集合 S 的幂集，$\langle \mathscr{P}(S), \subseteq\rangle$ 是一个偏序集。由于 $\mathscr{P}(S)$ 中的任意两个元素 S_1, S_2，它们的最大下界为 $S_1 \cap S_2$，最小上界为 $S_1 \cup S_2$，所以 $\langle \mathscr{P}(S), \subseteq\rangle$ 是格。

定义 6-1.2 设 $\langle A, \preccurlyeq\rangle$ 是一个格，如果在 A 上定义两个二元运算 $\vee$ 和 $\wedge$，使得对于任意的 $a, b \in A$，$a \vee b$ 等于 a 和 b 的最小上界，$a \wedge b$ 等于 a 和 b 的最大下界，那么，就称 $\langle A, \vee, \wedge\rangle$ 为由格 $\langle A, \preccurlyeq\rangle$ 所诱导的代数系统。二元运算 $\vee$ 和 $\wedge$ 分别称为并运算和交运算。

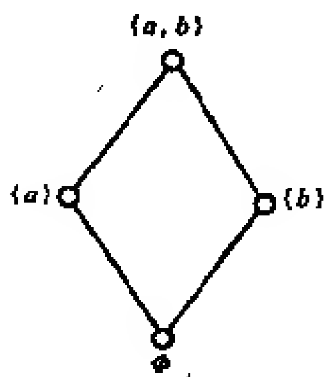


图 6-1.3

例 3 给定 $S=\{a, b\}$，$\mathscr{P}(S)=\{\phi, \{a\}, \{b\}, \{a, b\}\}$，那么，格 $\langle \mathscr{P}(S), \subseteq\rangle$ 如图 6-1.3 所示。

而由格 $\langle \mathscr{P}(S), \subseteq\rangle$ 所诱导的代数系统为 $\langle \mathscr{P}(S), \vee, \wedge\rangle$，其中运算 $\vee$ 是集合的并，运算 $\wedge$ 是集合的交。故 $\vee$ 和 $\wedge$ 的运算表可分别由表 6-1.1 的 (a) 和 (b) 所示。

定义 6-1.3 设 $\langle A, \preccurlyeq\rangle$ 是一个格，由 $\langle A, \preccurlyeq\rangle$ 诱导的代数系统为 $\langle A, \vee, \wedge\rangle$，设 $B \subseteq A$ 且 $B \neq \phi$，如果 A 中的这两个运算 $\vee$ 和 $\wedge$ 关于 B 是封闭的，则称 $\langle B, \preccurlyeq\rangle$ 是 $\langle A, \preccurlyeq\rangle$ 的子格。

可以证明子格必成为格。

表 6-1.1

(a)

$\vee$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

(b)

$\wedge$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

例 4　例 1 给出了一个具体的格 $\langle I_+, |\rangle$，由它诱导的代数系统为 $\langle I_+, \vee, \wedge\rangle$，其中 $a\vee b$ 就是 a，b 的最小公倍数，$a\wedge b$ 就是 a，b 的最大公约数。因为任何两个偶数的最大公约数和最小公倍数都是偶数，所以，如果取 E_+ 是正偶整数的全体，那么 $\vee$ 和 $\wedge$ 关于 E_+ 是封闭的，因此 $\langle E_+, |\rangle$ 是 $\langle I_+, |\rangle$ 的子格。

必须指出，对于格 $\langle A, \preccurlyeq\rangle$，设 B 是 A 的非空子集，尽管 $\langle B, \preccurlyeq\rangle$ 必定是一个偏序集，然而 $\langle B, \preccurlyeq\rangle$ 不一定是格，而且即使 $\langle B, \preccurlyeq\rangle$ 是格，也不一定是 $\langle A, \preccurlyeq\rangle$ 的子格。

例 5　设 $\langle S, \preccurlyeq\rangle$ 是一个格，其中

$$S=\{a, b, c, d, e, f, g, h\},$$

如图 6-1.4 所示。取

$$S_1=\{a, b, d, f\}$$

$$S_2=\{c, e, g, h\}$$

$$S_3=\{a, b, c, d, e, g, h\}$$

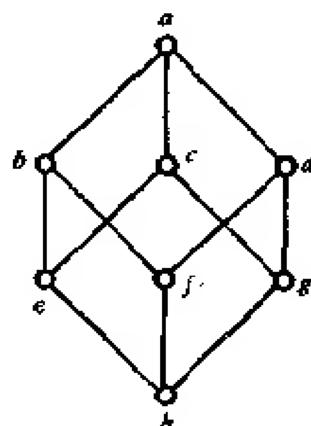


图 6-1.4

从图 6-1.4 上容易看出，$\langle S_1, \preccurlyeq\rangle$ 和 $\langle S_2, \preccurlyeq\rangle$ 都是 $\langle S, \preccurlyeq\rangle$ 的子格，而 $\langle S_3, \preccurlyeq\rangle$ 虽然是格，但它不是 $\langle S, \preccurlyeq\rangle$

的子格，这是因为

$$b \wedge d = f \notin S_3$$

例题1 设 $\langle S, \preccurlyeq \rangle$ 是一个格，任取 $a \in S$，构造 S 的子集 T 为：

$$T = \{x | x \in S \quad 且 \quad x \preccurlyeq a\}$$

则 $\langle T, \preccurlyeq \rangle$ 是 $\langle S, \preccurlyeq \rangle$ 的一个子格。

解 对于任意的 $x, y \in T$，必有 $x \preccurlyeq a$ 和 $y \preccurlyeq a$，

所以 $$x \vee y \preccurlyeq a, \quad x \wedge y \preccurlyeq a$$

故 $$x \vee y \in T, \quad x \wedge y \in T$$

因此，$\langle T, \preccurlyeq \rangle$ 是 $\langle S, \preccurlyeq \rangle$ 的一个子格。

同样地，可以证明，如果取 $Q = \{x | x \in S \text{ 且 } a \preccurlyeq x\}$，则 $\langle Q, \preccurlyeq \rangle$ 也是 $\langle S, \preccurlyeq \rangle$ 的一个子格。

在讨论格以及格所诱导的代数系统的一些性质之前，先介绍格的对偶原理。对偶这个概念在日常生活中也是屡见不鲜的，譬如，在不同国家的交通规则可能不同，但基本上是两种，一种是以左为准，另一种是以右为准，那么，在以左为准的交通规则中，如果将左换成右，右换成左就可得到另一种以右为准的交通规则，这里，左和右就是一种对偶概念。设 $\langle A, \preccurlyeq \rangle$ 是一个偏序集，在 A 上定义一个二元关系 $\preccurlyeq_R$，使得对于 A 中的两个元素 a, b 有关系 $a \preccurlyeq_R b$ 当且仅当 $b \preccurlyeq a$，不难看出 $\langle A, \preccurlyeq_R \rangle$ 也是一个偏序集。我们把偏序集 $\langle A, \preccurlyeq \rangle$ 和 $\langle A, \preccurlyeq_R \rangle$ 称为是彼此对偶的（互为对偶的），显然，它们所对应的哈斯图是互为颠倒的。容易证明：若 $\langle A, \preccurlyeq \rangle$ 是一个格，则 $\langle A, \preccurlyeq_R \rangle$ 也是一个格。我们把二元关系 $\preccurlyeq_R$ 称为二元关系 $\preccurlyeq$ 的逆关系，为简单起见，用记号 $\succcurlyeq$ 表示 $\preccurlyeq_R$。因为由格 $\langle A, \preccurlyeq \rangle$ 所定义的代数系统的并（交）运算正好是由格 $\langle A, \succcurlyeq \rangle$ 所定义的代数系统的交（并）运算，所以，关于格的对偶原理可以表述如下：

设 P 是对任意格都为真的命题，如果在命题 P 中把 $\preccurlyeq$ 换成 $\succcurlyeq$，$\vee$ 换成 $\wedge$，$\wedge$ 换成 $\vee$，就得到另一个命题 P'，我们把 P' 称为 P 的对偶命题，则 P' 对任意格也是真的命题。

下面，讨论一些格的基本性质。

定理 6-1.1 在一个格 $\langle A, \preccurlyeq\rangle$ 中，对任意的 $a, b\in A$，都有

$$a\preccurlyeq a\vee b, \qquad b\preccurlyeq a\vee b$$

$$a\wedge b\preccurlyeq a, \qquad a\wedge b\preccurlyeq b$$

证明 因为 a 和 b 的并是 a 的一个上界，所以

$$a\preccurlyeq a\vee b$$

同理

$$b\preccurlyeq a\vee b$$

由对偶原理，即得

$$a\wedge b\preccurlyeq a, \ a\wedge b\preccurlyeq b$$

□

定理 6-1.2 在一个格 $\langle A, \preccurlyeq\rangle$ 中，对于 $a, b, c, d\in A$，如果

$$a\preccurlyeq b \quad 和 \quad c\preccurlyeq d$$

则

$$a\vee c\preccurlyeq b\vee d$$

$$a\wedge c\preccurlyeq b\wedge d$$

证明 因为 $b\preccurlyeq b\vee d$, $d\preccurlyeq b\vee d$，所以，由传递性可得

$$a\preccurlyeq b\vee d, \ c\preccurlyeq b\vee d$$

这就表明 $b\vee d$ 是 a 和 c 的一个上界，而 $a\vee c$ 是 a 和 c 的最小上界，所以，必有

$$a\vee c\preccurlyeq b\vee d$$

类似地可以证明 $a\wedge c\preccurlyeq b\wedge d$ □

推论 在一个格 $\langle A, \preccurlyeq\rangle$ 中，对于 $a, b, c\in A$，如果 $b\preccurlyeq c$，则 $a\vee b\preccurlyeq a\vee c$, $a\wedge b\preccurlyeq a\wedge c$。这个性质称为格的保序性。

证明 只要在定理 6-1.2 中将 a 代替 b，b 代替 c，c 代替 d，即可得证。 □

定理 6-1.3 设 $\langle A, \preccurlyeq\rangle$ 是一个格，由格 $\langle A, \preccurlyeq\rangle$ 所诱导的代数系统为 $\langle A, \vee, \wedge\rangle$，则对任意的 $a, b, c, d\in A$，有

(1) $\left.\begin{array}{l} a\vee b=b\vee a \\ a\wedge b=b\wedge a \end{array}\right\}$（交换律）

(2) $\left.\begin{array}{l} a\vee(b\vee c)=(a\vee b)\vee c \\ a\wedge(b\wedge c)=(a\wedge b)\wedge c \end{array}\right\}$（结合律）

(3) $\left.\begin{array}{l} a\vee a=a \\ a\wedge a=a \end{array}\right\}$（幂等律）

(4) $\left.\begin{aligned} a\vee(a\wedge b)=a \\ a\wedge(a\vee b)=a \end{aligned}\right\}$（吸收律）

证明 (1) 格中任何两个元素 a, b 的最小上界(最大下界)当然等于 b, a 的最小上界(最大下界)，故

$$a\vee b=b\vee a \quad (a\wedge b=b\wedge a)$$

(2) 由定理 6-1.1 可知

$$b\preccurlyeq b\vee c\preccurlyeq a\vee(b\vee c) \quad 和 \quad a\preccurlyeq a\vee(b\vee c)$$

由定理 6-1.2，就有

$$(a\vee b)\preccurlyeq a\vee(b\vee c)$$

又因 $$c\preccurlyeq b\vee c\preccurlyeq a\vee(b\vee c)$$

再由定理 6-1.2，即得

$$(a\vee b)\vee c\preccurlyeq a\vee(b\vee c)$$

类似地可以证明

$$a\vee(b\vee c)\preccurlyeq(a\vee b)\vee c$$

因此 $$a\vee(b\vee c)=(a\vee b)\vee c$$

利用对偶原理，即得

$$a\wedge(b\wedge c)=(a\wedge b)\wedge c$$

(3) 由定理 6-1.1 可得 $a\preccurlyeq a\vee a$

由自反性可知 $$a\preccurlyeq a$$

由此可得 $$a\vee a\preccurlyeq a$$

因此 $$a\vee a=a$$

利用对偶原理，即得

$$a\wedge a=a$$

(4) 由定理 6-1.1 可得

$$a\preccurlyeq a\vee(a\wedge b)$$

因为 $$a\preccurlyeq a \quad 和 \quad a\wedge b\preccurlyeq a$$

所以 $$a\vee(a\wedge b)\preccurlyeq a$$

因此 $$a\vee(a\wedge b)=a$$

利用对偶原理，即得

$$a\wedge(a\vee b)=a$$

□

例 6 设 $\langle N, \leqslant\rangle$ 是一个偏序集合，这里 N 是自然数集，$\leqslant$ 是普通的数与数之间的“小于等于”关系，因为对于任意的 $a, b \in N$，有

$$a \vee b = \max(a, b)$$

$$a \wedge b = \min(a, b)$$

所以，$\langle N, \leqslant\rangle$ 是一个格，由这个格所诱导的代数系统是 $\langle N, \vee, \wedge\rangle$。

在此代数系统中，任意两个数 a 和 b 的最大值（最小值）与 b 和 a 的最大值（最小值）是相等的，因此，并运算和交运算都是可交换的；又因为 $\max(\max(a, b), c)$ 和 $\max(a, \max(b, c))$ 都是三个数 a, b, c 中的最大值，所以在 $\langle N, \vee, \wedge\rangle$ 中并运算是可结合的，同理，$\min(\min(a, b), c) = \min(a, \min(b, c))$，说明交运算的可结合性；由于 $\max(a, a) = \min(a, a) = a$，所以幂等性成立；又由于 $\max(a, \min(a, b)) = a$ 和 $\min(a, \max(a, b)) = a$，因此，吸收性也成立。

引理 6-1.1 设 $\langle A, \vee, \wedge\rangle$ 是一个代数系统，其中 $\vee$，$\wedge$ 都是二元运算且满足吸收性，则 $\vee$ 和 $\wedge$ 都满足幂等性。

证明 因为运算 $\vee$ 和 $\wedge$ 满足吸收性，即对任意的 $a, b \in A$，有

$$a \vee (a \wedge b) = a \tag{1}$$

$$a \wedge (a \vee b) = a \tag{2}$$

将(1)式中的 b 取为 $a \vee b$，便得

$$a \vee (a \wedge (a \vee b)) = a$$

再由(2)，即得

$$a \vee a = a$$

同理可证 $a \wedge a = a$ □

定理 6-1.4 设 $\langle A, \vee, \wedge\rangle$ 是一个代数系统，其中 $\vee$ 和 $\wedge$ 都是二元运算且满足交换性、结合性和吸收性，则 A 上存在偏序关系 $\preccurlyeq$，使 $\langle A, \preccurlyeq\rangle$ 是一个格。

证明 设在 A 上定义二元关系 $\preccurlyeq$ 为：对于任意 $a, b \in A$，

$a \preccurlyeq b$ 当且仅当

$$a \wedge b = a$$

首先证明二元关系 $\preccurlyeq$ 是一个偏序关系。

由引理 6-1.1 可知 $\wedge$ 必满足幂等性，即对任一 $a \in A$ 有 $a \wedge a = a$，所以 $a \preccurlyeq a$，故 $\preccurlyeq$ 是自反的。

设 $a \preccurlyeq b$，则 $a = a \wedge b$，再设 $b \preccurlyeq a$，则

$$b = b \wedge a$$

因为 $\wedge$ 满足交换律，因此，$a = b$，故 $\preccurlyeq$ 是反对称的。

设 $a \preccurlyeq b$，$b \preccurlyeq c$，则 $a \wedge b = a$，$b \wedge c = b$，因为

$$\begin{aligned} a \wedge c &= (a \wedge b) \wedge c \\ &= a \wedge (b \wedge c) \\ &= a \wedge b \\ &= a \end{aligned}$$

所以，$a \preccurlyeq c$，故 $\preccurlyeq$ 是传递的。因此，$\preccurlyeq$ 是偏序关系。

其次证明 $a \wedge b$ 是 a 和 b 的最大下界。

由于
$$(a \wedge b) \wedge a = a \wedge b$$
$$(a \wedge b) \wedge b = a \wedge b$$

所以，$a \wedge b \preccurlyeq a$，$a \wedge b \preccurlyeq b$，即 $a \wedge b$ 是 a 和 b 的下界。

设 c 是 a 和 b 的任一下界，即 $c \preccurlyeq a$，$c \preccurlyeq b$，那么就有

$$c \wedge a = c, \quad c \wedge b = c$$

而
$$c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$$

所以
$$c \preccurlyeq a \wedge b$$

这就证明了 $a \wedge b$ 是 a 和 b 的最大下界。

最后，根据交换性和吸收性，由 $a \wedge b = a$ 可得

$$(a \wedge b) \vee b = a \vee b$$

即
$$b = a \vee b$$

反之，由 $a \vee b = b$ 可得

$$a \wedge (a \vee b) = a \wedge b$$

即
$$a = a \wedge b$$

因此
$$a \wedge b = a \Leftrightarrow a \vee b = b$$

由此可知，A 上偏序关系即为：对任意的 $a, b\in A$; $a\preccurlyeq b$ 当且仅当 $a\vee b=b$，那么，就可以用类似的方法证明 $a\vee b$ 是 a 和 b 的最小上界。

因此，$\langle A, \preccurlyeq\rangle$ 是一个格。 □

定理 6-1.5 在一个格 $\langle A, \preccurlyeq\rangle$ 中，对任意的 $a, b, c\in A$，都有

$$a\vee(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c)$$
$$(a\wedge b)\vee(a\wedge c)\preccurlyeq a\wedge(b\vee c)$$

证明 由定理 6-1.1 可知 $a\preccurlyeq a\vee b$ 和 $a\preccurlyeq a\vee c$，由定理 6-1.2 和幂等性可得

$$a=a\wedge a\preccurlyeq(a\vee b)\wedge(a\vee c) \tag{1}$$

另外，由于 $b\wedge c\preccurlyeq b\preccurlyeq a\vee b$ 和 $b\wedge c\preccurlyeq c\preccurlyeq a\vee c$

所以

$$b\wedge c=(b\wedge c)\wedge(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c) \tag{2}$$

对于(1)式和(2)式，应用定理 6-1.2 即得

$$a\vee(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c)$$

利用对偶原理，即得

$$(a\wedge b)\vee(a\wedge c)\preccurlyeq a\wedge(b\vee c)$$ □

定理 6-1.6 设 $\langle A, \preccurlyeq\rangle$ 是一个格，那么，对于任意的 $a, b\in A$，有

$$a\preccurlyeq b\Leftrightarrow a\wedge b=a\Leftrightarrow a\vee b=b$$

证明 首先证明 $a\preccurlyeq b\Leftrightarrow a\wedge b=a$

由 $a\preccurlyeq b$ 和 $a\preccurlyeq a$，就有 $a\preccurlyeq a\wedge b$，但根据 $a\wedge b$ 的定义应有 $a\wedge b\preccurlyeq a$，由反对称性，得 $a\wedge b=a$，这就证明了 $a\preccurlyeq b\Rightarrow a\wedge b=a$。

反之，假定 $a\wedge b=a$，则 $a=a\wedge b\preccurlyeq b$，这就证明了

$$a\wedge b=a\Rightarrow a\preccurlyeq b$$

因此 $$a\preccurlyeq b\Leftrightarrow a\wedge b=a$$

用同样的方法，可以证明 $a\preccurlyeq b\Leftrightarrow a\vee b=b$，而 $a\wedge b=a\Leftrightarrow a\vee b=b$ 已经在定理 6-1.4 的证明过程中证过，这里不再重述。 □

定理 6-1.7 设 $\langle A, \preccurlyeq\rangle$ 是一个格，那么，对于任意的

$a, b, c \in A$，有

$$a \preccurlyeq c \Leftrightarrow a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$$

证明　由定理6-1.6有

$$a \preccurlyeq c \Leftrightarrow (a \vee c) = c$$

由定理6-1.5有

$$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$$

用 c 去代替上式中的 $(a \vee c)$，即得

$$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$$

所以 $$a \preccurlyeq c \Rightarrow a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$$

另外，若 $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$，则明显地有

$$a \preccurlyeq a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c \preccurlyeq c$$

即有 $$a \preccurlyeq c$$

所以 $$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c \Rightarrow a \preccurlyeq c$$

因此 $$a \preccurlyeq c \Leftrightarrow a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$$ □

推论　在一个格 $\langle A, \preccurlyeq \rangle$ 中，对任意的 $a, b, c \in A$，必有

$$(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee (a \wedge c))$$

和 $$a \vee (b \wedge (a \vee c)) \preccurlyeq (a \vee b) \wedge (a \vee c)$$

证明　利用 $a \wedge c \preccurlyeq a$ 和 $a \preccurlyeq a \vee c$，便可分别得证。□

定义6-1.4　设 $\langle A_1, \preccurlyeq_1 \rangle$ 和 $\langle A_2, \preccurlyeq_2 \rangle$ 是两个格，由它们分别诱导的代数系统为 $\langle A_1, \vee_1, \wedge_1 \rangle$ 和 $\langle A_2, \vee_2, \wedge_2 \rangle$，如果存在着一个从 A_1 到 A_2 的映射 f，使得对于任意的 $a, b \in A_1$，有

$$f(a \vee_1 b) = f(a) \vee_2 f(b)$$
$$f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

则称 f 为从 $\langle A_1, \vee_1, \wedge_1 \rangle$ 到 $\langle A_2, \vee_2, \wedge_2 \rangle$ 的格同态，亦可称 $\langle f(A_1), \preccurlyeq_2 \rangle$ 是 $\langle A_1, \preccurlyeq_1 \rangle$ 的格同态象。此外，当 f 是双射时，则称 f 为从 $\langle A_1, \vee_1, \wedge_1 \rangle$ 到 $\langle A_2, \vee_2, \wedge_2 \rangle$ 的格同构，亦称 $\langle A_1, \preccurlyeq_1 \rangle$ 和 $\langle A_2, \preccurlyeq_2 \rangle$ 这两个格是同构的。

定理6-1.8　设 f 是格 $\langle A_1, \preccurlyeq_1 \rangle$ 到 $\langle A_2, \preccurlyeq_2 \rangle$ 的格同态，则对任意的 $x, y \in A_1$，如果 $x \preccurlyeq_1 y$，必有 $f(x) \preccurlyeq_2 f(y)$。

证明　因为 $x \preccurlyeq_1 y$，所以　$x \wedge_1 y = x$

$$f(x\wedge_1 y)=f(x)$$

$$f(x)\wedge_2 f(y)=f(x)$$

故 $$f(x)\preccurlyeq_2 f(y)$$ □

定理 6-1.8 告诉我们格同态是保序的。但是定理 6-1.8 的逆命题是不一定成立的。如下例所述。

例 7 设 $\langle S, \preccurlyeq\rangle$ 是一个格，其中

$$S=\{a, b, c, d, e\}$$

如图 6-1.5 所示。

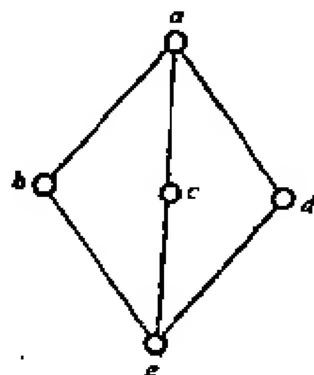


图 6-1.5

我们知道，$\langle \mathscr{P}(S), \subseteq\rangle$ 也是一个格，作映射 $f: S\to\mathscr{P}(S)$，对任一 $x\in S$，使得

$$f(x)=\{y\mid y\in S,\ y\preccurlyeq x\}$$

即有

$$f(a)=S,\ f(b)=\{b, e\},\ f(c)=\{c, e\}$$

$$f(d)=\{d, e\},\ f(e)=\{e\}$$

显然，当 x, $y\in S$ 且 $x\preccurlyeq y$ 时，有 $f(x)\subseteq f(y)$，所以 f 是保序的。但是，对于 b, $d\in S$，有

$$b\vee d=a$$

$$f(b\vee d)=f(a)=S$$

而 $$f(b)\cup f(d)=\{b, d, e\}$$

所以 $$f(b\vee d)\neq f(b)\cup f(d)$$

定理 6-1.9 设两个格为 $\langle A_1, \preccurlyeq_1\rangle$ 和 $\langle A_2, \preccurlyeq_2\rangle$，$f$ 是从 A_1 到 A_2 的双射，则 f 是 $\langle A_1, \preccurlyeq_1\rangle$ 到 $\langle A_2, \preccurlyeq_2\rangle$ 的格同构，当且仅当对任意的 a, $b\in A_1$, $a\preccurlyeq_1 b\Leftrightarrow f(a)\preccurlyeq_2 f(b)$。

证明 设 f 是 $\langle A_1, \preccurlyeq_1\rangle$ 到 $\langle A_2, \preccurlyeq_2\rangle$ 的格同构。由定理 6-1.8 可知，如果对任意的 a, $b\in A_1$, $a\preccurlyeq_1 b$ 则 $f(a)\preccurlyeq_2 f(b)$，反之，设 $f(a)\preccurlyeq_2 f(b)$，则 $f(a)\wedge_2 f(b)=f(a\wedge_1 b)=f(a)$，由于 f 是双射，所以 $a\wedge_1 b=a$，故 $a\preccurlyeq_1 b$。

设对任意的 a, $b\in A_1$, $a\preccurlyeq_1 b\Leftrightarrow f(a)\preccurlyeq_2 f(b)$，设 $a\wedge_1 b=c$，则 $c\preccurlyeq_1 a$, $c\preccurlyeq_1 b$，于是，

$$f(a\wedge_1 b)=f(c),\quad f(c)\preccurlyeq_2 f(a),\quad f(c)\preccurlyeq_2 f(b)$$

故有 $$f(c) \preccurlyeq_2 f(a) \wedge_2 f(b)$$

设 $$f(a) \wedge_2 f(b) = f(d)$$

则 $$f(c) \preccurlyeq_2 f(d),\ f(d) \preccurlyeq_2 f(a),\ f(d) \preccurlyeq_2 f(b)$$

故有 $d \preccurlyeq_1 a$, $d \preccurlyeq_1 b$, 于是, $d \preccurlyeq_1 a \wedge_1 b$ 即 $d \preccurlyeq_1 c$, 所以

$$f(d) \preccurlyeq_2 f(c)$$

因此 $$f(c) = f(d)$$

即 $$f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

类似地可证 $$f(a \vee_1 b) = f(a) \vee_2 f(b)$$

因此, f 是 $\langle A_1, \preccurlyeq_1 \rangle$ 到 $\langle A_2, \preccurlyeq_2 \rangle$ 的格同构。 □

6-1 习题

(1) 由图 6-1.6 所示的偏序集, 哪一个是格? 为什么?

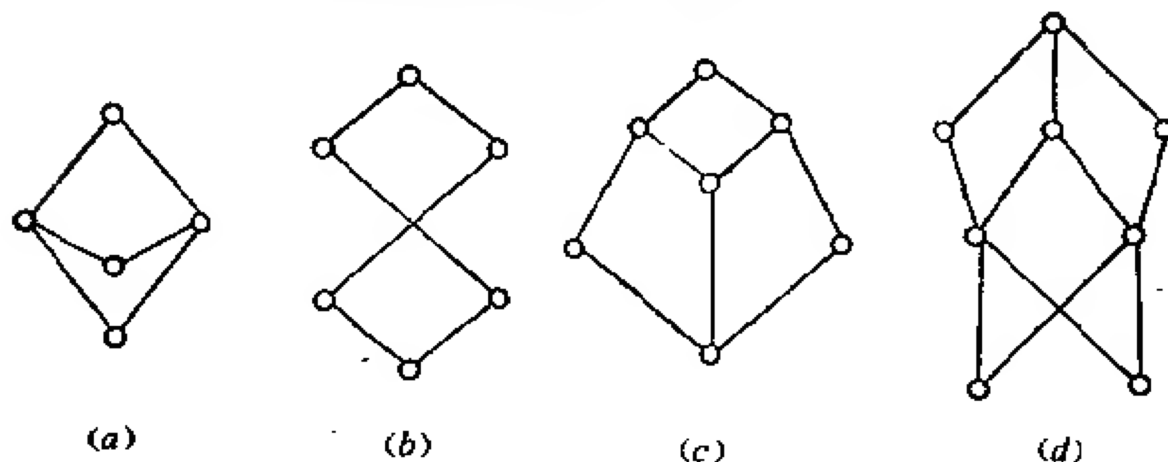


图 6-1.6

(2) 由下列集合 L 构成的偏序集 $\langle A, \preccurlyeq \rangle$, 其中 $\preccurlyeq$ 定义为: 对于 $n_1, n_2 \in L$, $n_1 \preccurlyeq n_2$ 当且仅当 n_1 是 n_2 的因子。问其中哪几个偏序集是格。

a) $L = \{1, 2, 3, 4, 6, 12\}$

b) $L = \{1, 2, 3, 4, 6, 8, 12, 14\}$

c) $L = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

(3) 验证以整除关系"|"为偏序关系的正整数格 $\langle I^+, | \rangle$ 所诱导的代数系统 $\langle I^+, \vee, \wedge \rangle$ 满足 $\vee$, $\wedge$ 的交换性、结合性、等幂性以及吸收性。

(4) 设 $\langle A, \preccurlyeq \rangle$ 是一个格, 任取 a, b 且 $a \prec b$[注], 构造集合

$$B = \{x \mid x \in A \text{ 且 } a \preccurlyeq x \preccurlyeq b\}$$

则 $\langle B, \preccurlyeq \rangle$ 也是一个格。

[注] $a \prec b$ 意指 $a \preccurlyeq b$ 且 $a \neq b$。

(5) 设 A, B 是两个集合, f 是 A 到 B 的映射, 证明 $\langle S, \subseteq\rangle$ 是 $\langle \mathscr{P}(B), \subseteq\rangle$ 的一个子格, 其中

$$S=\{y \mid y=f(x),\ x\in \mathscr{P}(A)\}。$$

(6) 设 $\langle A, \vee, \wedge\rangle$ 是一个代数系统, 其中 $\vee$, $\wedge$ 都是二元运算且分别满足幂等性, 试举例说明吸收性不一定成立。

(7) 设 a 和 b 是格 $\langle A, \preccurlyeq\rangle$ 中的两个元素, 证明

a) $a\wedge b=b$ 当且仅当 $a\vee b=a$;

b) $a\wedge b\prec b$ 和 $a\wedge b\prec a$ 当且仅当 a 与 b 是不可比较的。

(8) 证明在格中若 $a\preccurlyeq b\preccurlyeq c$, 则

$$a\vee b=b\wedge c$$

$$(a\wedge b)\vee(b\wedge c)=b=(a\vee b)\wedge(a\vee c)$$

(9) 证明在格中成立

$$(a\wedge b)\vee(c\wedge d)\preccurlyeq(a\vee c)\wedge(b\vee d)$$

和 $$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)\preccurlyeq(a\vee b)\wedge(b\vee c)\wedge(c\vee a)$$

(10) 用对偶原理证明定理 6-1.2 中的后一个结论, 即在格中若 $a\preccurlyeq b$ 和 $c\preccurlyeq d$, 则 $a\wedge c\preccurlyeq b\wedge d$。

(11) 设 $\langle A, \preccurlyeq\rangle$ 是一个格, 证明 $\langle A, \preccurlyeq_R\rangle$ 也是一个格。

6-2 分 配 格

在定理 6-1.5 中我们已经证明, 在格 $\langle A, \preccurlyeq\rangle$ 中的任意元素 a, b, c, 必有

$$a\vee(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c)$$

和

$$(a\wedge b)\vee(a\wedge c)\preccurlyeq a\wedge(b\vee c)$$

成立。当上述两个式子中的等号成立的时候, 我们就得到一类特殊的格。

定义 6-2.1 设 $\langle A, \vee, \wedge\rangle$ 是由格 $\langle A, \preccurlyeq\rangle$ 所诱导的代数系统。如果对任意的 a, b, $c\in A$, 满足

$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$$

(交运算对于并运算可分配)

和

$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)$$

(并运算对于交运算可分配)

则称 $\langle A, \preccurlyeq\rangle$ 是分配格。

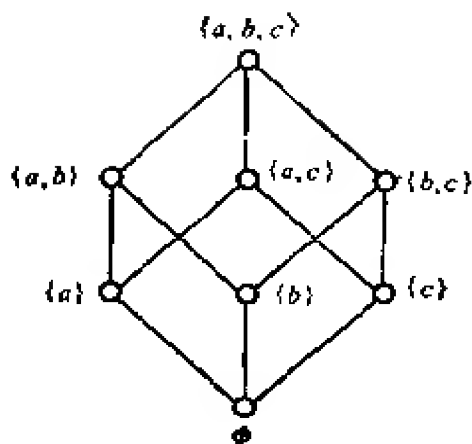


图 6-2.1

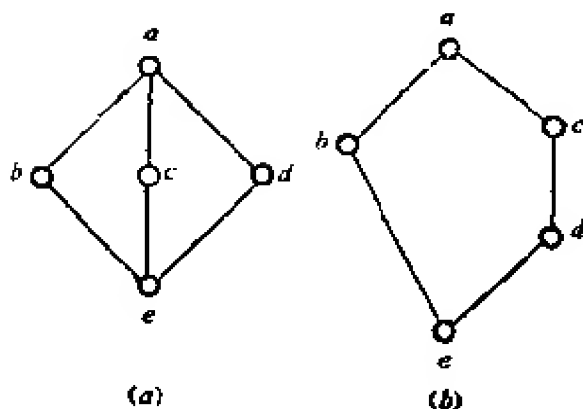


图 6-2.2

例 1 设 $S=\{a, b, c\}$, 则 $\langle\mathscr{P}(S), \cup, \cap\rangle$ 是由格 $\langle\mathscr{P}(S), \subseteq\rangle$ 所诱导的代数系统。这个格所对应的哈斯图如图 6-2.1 所示。

容易验证, 对于任意的 $P, Q, R\in\mathscr{P}(S)$, 有

$$P\cap(Q\cup R)=(P\cap Q)\cup(P\cap R)$$
$$P\cup(Q\cap R)=(P\cup Q)\cap(P\cup R)$$

成立。所以, $\langle\mathscr{P}(S), \subseteq\rangle$ 是一个分配格。

例 2 如图 6-2.2 中所示的两个格都不是分配格。

这是因为, 在图 6-2.2 (a) 中, $b\wedge(c\vee d)=b\wedge a=b$

而 $$(b\wedge c)\vee(b\wedge d)=e\vee e=e$$

所以 $$b\wedge(c\vee d)\neq(b\wedge c)\vee(b\wedge d)$$

在图 6-2.2 (b) 中,

$$c\wedge(b\vee d)=c\wedge a=c$$

而 $$(c\wedge b)\vee(c\wedge d)=e\vee d=d$$

所以 $$c\wedge(b\vee d)\neq(c\wedge b)\vee(c\wedge d)$$

必须指出, 在分配格的定义中, 必须是对任意的 $a, b, c\in A$ 都要满足分配等式, 因此, 决不能验证格中的某些元素满足分配等式就断定该格是分配格。譬如, 在例 2 中, 图 6-2.2(b) 所示的格中, 尽管有

$$d\wedge(b\vee c)=d\wedge a=d=e\vee d=(d\wedge b)\vee(d\wedge c)$$
$$b\wedge(c\vee d)=b\wedge c=e=e\vee e=(b\wedge c)\vee(b\wedge d)$$

但它不是分配格。

例 2 中给出的两个具有五个元素的格是很重要的，因为有一个定理证明了如下的结论：一个格是分配格的充要条件是在该格中没有任何子格与这两个五元素格中的任一个同构。这个定理的证明已超出了本书的范围。

例 3 如图 6–2.3 中所示的格中，因为 $\langle\{a, b, d, g, c\}, \preccurlyeq\rangle$ 是格 $\langle\{a, b, c, d, e, f, g\}, \preccurlyeq\rangle$ 的子格，而这个子格是与图 6–2.2(b) 同构的，所以，图 6–2.3 所示的格不是分配格。

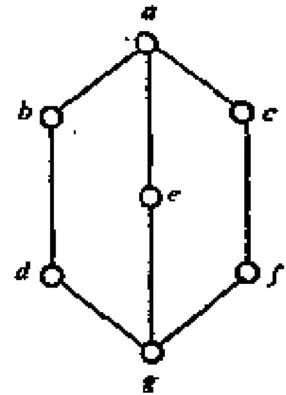


图 6-2.3

应该指出，在分配格的定义中，条件还可减弱，这就是两个分配等式是等价的。

定理 6-2.1 如果在一个格中交运算对于并运算可分配，则并运算对交运算也一定是可分配的。反之亦然。

证明 设格中任意元素 a, b, c，如果

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

那么

$$\begin{aligned}(a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \\ &= a \vee ((a \vee b) \wedge c) \\ &= a \vee ((a \wedge c) \vee (b \wedge c)) \\ &= (a \vee (a \wedge c)) \vee (b \wedge c) \\ &= a \vee (b \wedge c)\end{aligned}$$

用类似的方法可证，若

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

则

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

□

从例 2 中，我们已经看到一个格不一定是分配格，但是某些格一定是分配格，如以下的定理所述。

定理 6-2.2 每个链是分配格。

证明 设 $\langle A, \preccurlyeq\rangle$ 是一个链，所以，$\langle A, \preccurlyeq\rangle$ 一定是格。

对于任意的 $a, b, c \in A$，只要讨论以下两种可能的情况：

(1) $a \preccurlyeq b$ 或 $a \preccurlyeq c$

(2) $b \preccurlyeq a$ 且 $c \preccurlyeq a$

对于情况(1)，无论是 $b \preccurlyeq c$ 还是 $c \preccurlyeq b$，都有

$$a \wedge (b \vee c) = a \quad \text{和} \quad (a \wedge b) \vee (a \wedge c) = a$$

对于情况(2)，总有 $b \vee c \preccurlyeq a$

所以
$$a \wedge (b \vee c) = b \vee c$$

而由 $b \preccurlyeq a$ 和 $c \preccurlyeq a$，应有

$$(a \wedge b) \vee (a \wedge c) = b \vee c$$

故 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ 总成立。

因此，$\langle A, \preccurlyeq \rangle$ 是一个分配格。 □

定理 6-2.3 设 $\langle A, \preccurlyeq \rangle$ 是一个分配格，那么，对于任意的 $a, b, c \in A$，如果有

$$a \wedge b = a \wedge c \quad \text{和} \quad a \vee b = a \vee c$$

成立，则必有
$$b = c$$

证明 因为

$$(a \wedge b) \vee c = (a \wedge c) \vee c = c$$

而

$$\begin{aligned}(a \wedge b) \vee c &= (a \vee c) \wedge (b \vee c) = (a \vee b) \wedge (b \vee c) \\ &= b \vee (a \wedge c) = b \vee (a \wedge b) = b\end{aligned}$$

所以
$$b = c$$
□

定义 6-2.2 设 $\langle A, \preccurlyeq \rangle$ 是一个格，由它诱导的代数系统为 $\langle A, \vee, \wedge \rangle$，如果对于任意的 $a, b, c \in A$，当 $b \preccurlyeq a$ 时，有

$$a \wedge (b \vee c) = b \vee (a \wedge c)$$

则称 $\langle A, \preccurlyeq \rangle$ 是模格。

定理 6-2.4 格 $\langle A, \preccurlyeq \rangle$ 是模格，当且仅当在 A 中不含有适合下述条件的元素 u, v, w

$$v \prec u \quad \text{且} \quad u \vee w = v \vee w, \; u \wedge w = v \wedge w$$

证明 若 A 中含有满足上述条件的三个元素 u, v, w，因为 $v \prec u$ 且

$$u \wedge (w \vee v) = u \wedge (w \vee u) = u$$

$$(u\wedge w)\vee v=(v\wedge w)\vee v=v$$

故有 $$(u\wedge w)\vee v\prec u\wedge(w\vee v)$$

所以，$\langle A, \preccurlyeq\rangle$ 不是模格。

反之，若 $\langle A, \preccurlyeq\rangle$ 不是模格，则有适合

$$b\preccurlyeq a \quad 且 \quad b\vee(c\wedge a)\prec(b\vee c)\wedge a$$

的 a, b, c。

令 $$v=b\vee(c\wedge a),\ u=(b\vee c)\wedge a,\ w=c$$

有

$$\begin{aligned}u\wedge w&=((b\vee c)\wedge a)\wedge c\\&=a\wedge((b\vee c)\wedge c)\\&=a\wedge c\\&=(a\wedge c)\wedge c\end{aligned}$$

因此 $$u\wedge w\preccurlyeq v\wedge w$$

另外，由于 $$v\prec u$$

故有 $$v\wedge w\preccurlyeq u\wedge w$$

所以 $$u\wedge w=v\wedge w$$

同理可证 $$u\vee w=v\vee w$$

由此可见，若 $\langle A, \preccurlyeq\rangle$ 不是模格，就一定存在 u, v, $w\in A$，使得 $v\prec u$ 且

$$u\vee w=v\vee w,\quad u\wedge w=v\wedge w。$$ □

我们知道，在一般的格中，对于任意的 a, b, c, 有以下三个式子成立：

$$a\vee(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c) \tag{1}$$

$$(a\wedge b)\vee(a\wedge c)\preccurlyeq a\wedge(b\vee c) \tag{2}$$

$$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)\preccurlyeq(a\vee b)\wedge(b\vee c)\wedge(c\vee a) \tag{3}$$

定理 6-2.5 对于模格，若有三个元素 a, b, c, 使得上述三个式子的任何一个式子中把“$\preccurlyeq$”换成“$=$”成立，则另外两个式子中把“$\preccurlyeq$”换成“$=$”也必成立。

证明 设(1)的等号成立，则由对偶原理(2)的等号也成立。又因

$$
\begin{aligned}
(a\vee b)\wedge(b\vee c)\wedge(c\vee a) &= ((a\wedge c)\vee b)\wedge(c\vee a)\\
&= ((c\vee a)\wedge b)\vee(a\wedge c)\\
&= (a\wedge b)\vee(b\wedge c)\vee(c\wedge a)
\end{aligned}
$$

即(3)的等号也成立。

若(3)的等号成立，则有

$$
\begin{aligned}
a\vee(b\wedge c) &= a\vee(a\wedge b)\vee(c\wedge a)\vee(b\wedge c)\\
&= a\vee((a\vee b)\wedge(b\vee c)\wedge(c\vee a))\\
&= a\vee((b\vee c)\wedge((a\vee b)\wedge(c\vee a))\\
&= (a\vee b\vee c)\wedge(a\vee b)\wedge(c\vee a)\\
&= (a\vee b)\wedge(a\vee c)
\end{aligned}
$$ □

定理 6-2.6 分配格必定是模格。

证明 设 $\langle A, \preccurlyeq\rangle$ 是一个分配格，对于任意的 $a, b, c\in A$，如果 $b\preccurlyeq a$，则 $a\wedge b=b$。因此，

$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)=b\vee(a\wedge c)$$ □

6-2 习题

(1) 试举两个含有 6 个元素的格，其中一个是分配格，另一个不是分配格。

(2) 在图 6-2.4 中给出的几个格，哪个是分配格？

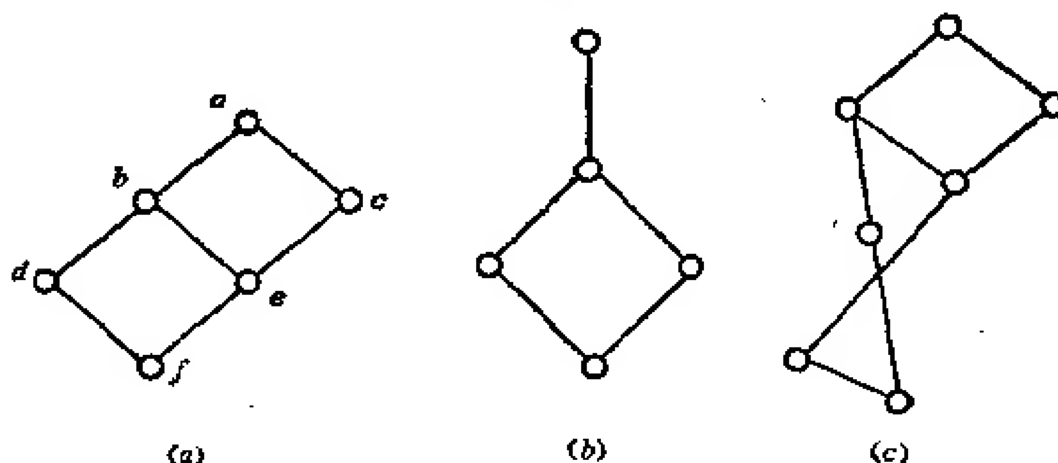


图 6-2.4

(3) 证明格 $\langle I, \max, \min\rangle$ 是分配格。

(4) 证明在分配格中，可把分配式更一般地写成

$$a\wedge(b_1\vee b_2\vee\cdots\vee b_n)=(a\wedge b_1)\vee(a\wedge b_2)\vee\cdots\vee(a\wedge b_n)$$

$$a \vee (b_1 \wedge b_2 \wedge \cdots \wedge b_n) = (a \vee b_1) \wedge (a \vee b_2) \wedge \cdots \wedge (a \vee b_n)$$

(5) 设 $\langle A, \preccurlyeq \rangle$ 是一个分配格，a, $b \in A$ 且 $a \prec b$, 证明

$$f(x) = (x \vee a) \wedge b$$

是一个从 A 到 B 的同态映射。其中

$$B = \{x \mid x \in A \quad 且 \quad a \preccurlyeq x \preccurlyeq b\}$$

(6) 试举例说明模格不一定是分配格。

*(7) 证明：一个格 $\langle A, \preccurlyeq \rangle$ 是分配格当且仅当对任意的 a, b, $c \in A$, 有

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$$

(8) 举出两个含有 6 个元素的格，其中一个是模格，另一个不是模格。

(9) 证明：一个格是模格当且仅当对于任意的 a, b, c, 有

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$$

(10) 设 $\langle A, \preccurlyeq \rangle$ 是模格，x, y, $a \in A$, 且 x, y 分别盖住 a, 证明 $x \vee y$ 盖住 x 和 y。

*(11) 设 $\langle S, \preccurlyeq \rangle$ 是模格，a, $b \in S$, 作 $X = \{x \mid x \in S$ 且 $a \wedge b \preccurlyeq x \preccurlyeq a\}$, $Y = \{y \mid y \in S$ 且 $b \preccurlyeq y \preccurlyeq a \vee b\}$, 则下面的互逆映射

$$x \to x \vee b \quad (x \in X)$$

$$y \to y \wedge a \quad (y \in Y)$$

是 X 和 Y 之间的同构。

6-3 有 补 格

在介绍有补格之前，先要介绍有界格。

定义 6-3.1 设 $\langle A, \preccurlyeq \rangle$ 是一个格，如果存在元素 $a \in A$, 对于任意的 $x \in A$, 都有

$$a \preccurlyeq x$$

则称 a 为格 $\langle A, \preccurlyeq \rangle$ 的全下界，记格的全下界为 0。

定理 6-3.1 一个格 $\langle A, \preccurlyeq \rangle$ 若有全下界，则是唯一的。

证明 用反证法。

如果有两个全下界 a 和 b, a, $b \in A$ 且 $a \neq b$, 因为 a 是全下界，$b \in A$, 所以 $a \preccurlyeq b$。同样地，因为 b 是全下界，$a \in A$, 所以 $b \preccurlyeq a$。

由此可得 $a = b$, 这与假设相矛盾。 □

定义 6-3.2 设 $\langle A, \preccurlyeq\rangle$ 是一个格，如果存在元素 $b \in A$，对于任意的 $x \in A$，都有

$$x \preccurlyeq b$$

则称 b 为格 $\langle A, \preccurlyeq\rangle$ 的全上界。记格的全上界为 **1**。

定理 6-3.2 一个格 $\langle A, \preccurlyeq\rangle$ 若有全上界，则是唯一的。

证明 与定理 6-3.1 的证法相类似。 □

例 1 设有限集合 S，那么在格 $\langle \mathscr{P}(S), \subseteq\rangle$ 中，空集 ϕ 就是该格的全下界，集合 S 就是该格的全上界。

例 2 在图 6-3.1 所示的格中，h 是全下界，a 是全上界。

定义 6-3.3 如果一个格中存在全下界和全上界，则称该格为有界格。

定理 6-3.3 设 $\langle A, \preccurlyeq\rangle$ 是一个有界格，则对任意的 $a \in A$，必有

$$a \vee 1 = 1 \qquad a \wedge 1 = a$$
$$a \vee 0 = a \qquad a \wedge 0 = 0$$

证明 因为 $a \vee 1 \in A$ 且 1 是全上界，所以 $a \vee 1 \preccurlyeq 1$，又因 $1 \preccurlyeq a \vee 1$，因此，$a \vee 1 = 1$。

因为 $a \preccurlyeq a$，$a \preccurlyeq 1$，所以 $a \preccurlyeq a \wedge 1$，又因 $a \wedge 1 \preccurlyeq a$，因此，

$$a \wedge 1 = a$$

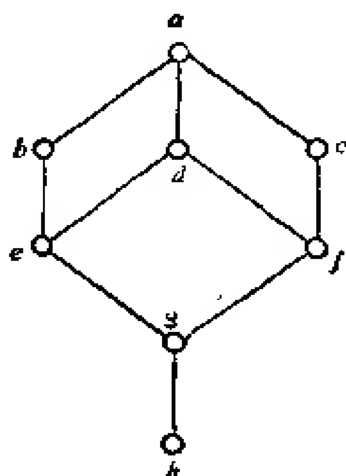


图 6-3.1

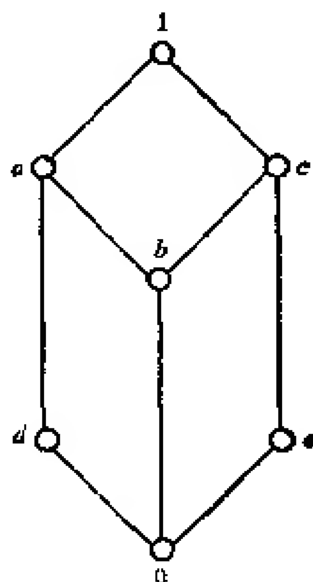


图 6-3.2

$a \vee 0 = a$ 和 $a \wedge 0 = 0$ 可以类似地进行证明。 □

由 $a \vee 0 = 0 \vee a = a$ 和 $a \wedge 1 = 1 \wedge a = a$ 说明 0 和 1 分别是关于运算 $\vee$ 和 $\wedge$ 的幺元。另外，0 和 1 分别是关于运算 $\wedge$ 和 $\vee$ 的零元。

定义 6-3.4 设 $\langle A, \preccurlyeq \rangle$ 是一个有界格，对于 A 中的一个元素 a，如果存在 $b \in A$，使得 $a \vee b = 1$ 和 $a \wedge b = 0$，则称元素 b 是元素 a 的补元。

显然，上述定义中，a 和 b 是对称的，即如果 a 是 b 的补元，则 b 也是 a 的补元，因此，可以说，a 和 b 这两个元素是互补的。必须注意的是：对于元素 $a \in A$，可以存在多个补元，也可以不存在补元。

例 3 在图 6-3.2 所示的有界格中，因为 $d \vee c = 1$ 和 $d \wedge c = 0$，所以，d 和 c 是互补的。但是 b 是没有补元的。此外，a 和 d 都是 e 的补元；c 和 e 都是 d 的补元。

显然，在有界格中，0 是 1 的唯一补元，1 是 0 的唯一补元。

定义 6-3.5 在一个有界格中，如果每个元素都至少有一个补元素，则称此格为有补格。

例 4 图 6-3.3 中给出了一些有补格。

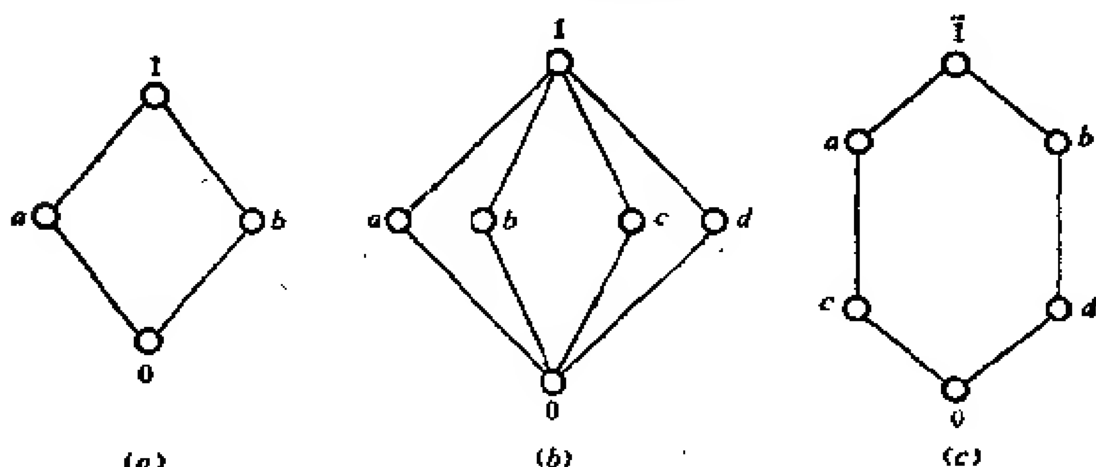


图 6-3.3

定理 6-3.4 在有界分配格中，若有一个元素有补元素，则必是唯一的。

证明 设 a 有两个补元素 b 和 c，即有

$$a\vee b=1 \qquad a\wedge b=0$$
$$a\vee c=1 \qquad a\wedge c=0$$

由定理 6-2.3 即得 $b=c$。

这就证明了 a 的补元素是唯一的。 □

定义 6-3.6 一个格如果它既是有补格，又是分配格，则称它为有补分配格。我们把有补分配格中任一元素 a 的唯一补元记为 $\bar{a}$。

6-3 习题

(1) 试根据图 6-3.4 所示的有界格，回答以下问题。

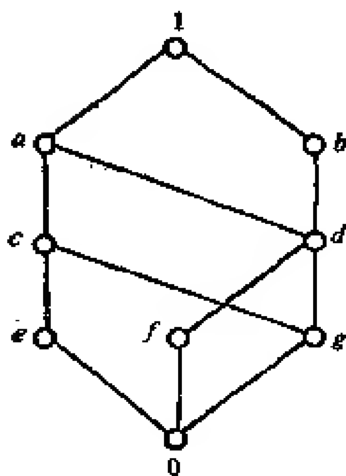


图 6-3.4

a) a 和 f 的补元素分别是哪些元素？

b) 该有界格是分配格吗？

c) 该有界格是有补格吗？

(2) 证明：在有界格中 0 是 1 的唯一补元，1 是 0 的唯一补元。

(3) 证明具有两个或更多个元素的格中不存在以自身为补元的元素。

(4) 在有界分配格中，证明具有补元的那些元素组成一个子格。

(5) 试证明：具有三个或更多个元素的链不是有补格。

(6) 设 $\langle A, \preccurlyeq\rangle$ 是一个有界格，对于 $x, y\in A$，证明

a) 若 $x\vee y=0$ 则 $x=y=0$

b) 若 $x\wedge y=1$ 则 $x=y=1$

6-4 布尔代数

一个非空集 S 的幂集 $\mathscr{P}(S)$，$\langle\mathscr{P}(S), \subseteq\rangle$ 作为一个格，已经在以前的讨论中多次出现。在这一节中，我们引进布尔代数，并将证明：任何一个有限布尔代数必定与一个格 $\langle\mathscr{P}(S), \subseteq\rangle$ 所诱导的代数系统同构。

定义 6-4.1 一个有补分配格称为布尔格。

设 $\langle A, \preccurlyeq\rangle$ 是一个布尔格，因为布尔格中的每一个元素 a 都有唯一的补元 $\bar{a}$，所以，我们就可以在 A 上确定一个一元运算，记为“$-$”，使得 $\bar{a}$ 为 a 的补元。我们把这个一元运算称为补运算，并把 a 和 b 的并(交)的补记为 $\overline{a\vee b}$($\overline{a\wedge b}$)。

定义 6-4.2 由布尔格 $\langle A, \preccurlyeq\rangle$，可以诱导一个代数系统 $\langle A, \vee, \wedge, ^{-}\rangle$，这个代数系统称为布尔代数。

例 1 设 S 是一个非空有限集，$\langle \mathscr{P}(S), \subseteq\rangle$ 是一个格，因为集合的交(并)对于并(交)是可分配的；$\langle \mathscr{P}(S), \subseteq\rangle$ 的全上界是 S，全下界是 $\emptyset$；对于任一集合 $T\subseteq S$，即任一 $T\in\mathscr{P}(S)$ 都有一个补元素 $S-T\in\mathscr{P}(S)$，所以 $\langle \mathscr{P}(S), \subseteq\rangle$ 是一个布尔格。由这个布尔格所诱导的代数系统 $\langle \mathscr{P}(S), \cup, \cap, \sim\rangle$ 是一个布尔代数。譬如，取 $S=\{a, b\}$，则 $\mathscr{P}(S)=\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$，由格 $\langle\{\emptyset, \{a\}, \{b\}, \{a, b\}\}, \subseteq\rangle$ 所诱导的代数系统为 $\langle\{\emptyset, \{a\}, \{b\}, \{a, b\}\}, \cup, \cap, \sim\rangle$，其运算如表 6-4.1 所示。

表 6-4.1

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

	$\sim$
$\emptyset$	$\{a, b\}$
$\{a\}$	$\{b\}$
$\{b\}$	$\{a\}$
$\{a, b\}$	$\emptyset$

定理 6-4.1 对于布尔代数中任意两个元素 a, b，必定有

$$\overline{(\bar{a})}=a$$

$$\overline{a\vee b}=\bar{a}\wedge\bar{b}$$

$$\overline{a\wedge b}=\bar{a}\vee\bar{b}$$

证明 由补元的定义可知，a 和 $\bar{a}$ 是互补的，就是说 $\bar{a}$ 的补元

是 a，所以 $\overline{(\overline{a})}=a$。由

$$(a\vee b)\vee(\overline{a}\wedge\overline{b})=((a\vee b)\vee\overline{a})\wedge((a\vee b)\vee\overline{b})$$
$$=(b\vee(a\vee\overline{a}))\wedge(a\vee(b\vee\overline{b}))$$
$$=(b\vee 1)\wedge(a\vee 1)=1\wedge 1=1$$

和

$$(a\vee b)\wedge(\overline{a}\wedge\overline{b})=(a\wedge(\overline{a}\wedge\overline{b}))\vee(b\wedge(\overline{a}\wedge\overline{b}))$$
$$=((a\wedge\overline{a})\wedge\overline{b})\vee((b\wedge\overline{b})\wedge\overline{a})$$
$$=(0\wedge\overline{b})\vee(0\wedge\overline{a})=0\vee 0=0$$

可知 $a\vee b$ 的补元为 $\overline{a}\wedge\overline{b}$。因为布尔代数中任一元素的补元是唯一的，所以

$$\overline{(a\vee b)}=\overline{a}\wedge\overline{b}$$

同理可知 $$\overline{(a\wedge b)}=\overline{a}\vee\overline{b}$$ □

定义 6-4.3 具有有限个元素的布尔代数称为有限布尔代数。

定义 6-4.4 设 $\langle A, \vee, \wedge, \bar{}\ \rangle$ 和 $\langle B, \vee, \wedge, \bar{}\ \rangle$ 是两个布尔代数，如果存在着 A 到 B 的双射 f，对于任意的 $a, b\in A$，都有

$$f(a\vee b)=f(a)\vee f(b)$$
$$f(a\wedge b)=f(a)\wedge f(b)$$
$$f(\overline{a})=\overline{f(a)}$$

则称 $\langle A, \vee, \wedge, \bar{}\ \rangle$ 和 $\langle B, \vee, \wedge, \bar{}\ \rangle$ 同构。

对于有限布尔代数，我们将证明以下的结论：对于每一正整数 n，必存在含有 2^n 个元素的布尔代数；反之，任一有限布尔代数，它的元素个数必为 2 的幂次。对于元素个数相同的布尔代数都是同构的。

为了证明这些结论，先介绍一些有关概念。

定义 6-4.5 设 $\langle A, \preccurlyeq\rangle$ 是一个格，且具有全下界 0，如果有元素 a 盖住 0，则称元素 a 为原子。

很明显，在格中若有原子 a, b 且 $a\neq b$，则必有 $a\wedge b=0$。

例 2 在图 6-4.1 所示的格中，d, e 都是原子且 $d\wedge e=0$，说明原子不是唯一的。1 盖住 a, b, c；a 盖住 d；c 盖住 e；b 盖住

d, e, 这说明一个元素可以盖住多个元素。

定理 6-4.2 设 $\langle A, \preccurlyeq\rangle$ 是一个具有全下界 0 的有限格，则对于任何一个非零元素 b（即不等于全下界 0 的元素）至少存在一个原子 a，使得 $a \preccurlyeq b$。

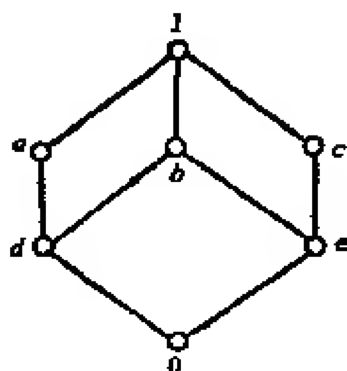


图 6-4.1

证明 如果 b 本身就是一个原子，那么，由 $b \preccurlyeq b$ 就得证。

如果 b 不是原子，那么必有 b_1，存在使得

$$0 \prec b_1 \prec b$$

如果 b_1 是原子，那么，定理得证。否则，必存在 b_2 使得

$$0 \prec b_2 \prec b_1 \prec b$$

由于 $\langle A, \preccurlyeq\rangle$ 是一个有下界的有限格，所以通过有限的步骤总可找到一个原子 b_i，使得

$$0 \prec b_i \prec \cdots \prec b_2 \prec b_1 \prec b$$

它是 $\langle A, \preccurlyeq\rangle$ 中的一条链，其中 b_i 是原子，且 $b_i \prec b$。 □

上述定理中的 b_i 不一定是唯一的。如图 6-4.1 中所示的有限格，对 a 有唯一的原子 d，使 $d \prec a$；对 c 有唯一的原子 e，使 $e \prec c$；对 b 就有两个原子 d 和 e，使 $d \prec b$ 和 $e \prec b$；对 1 同样有两个原于 d 和 e，使 $d \prec a \prec 1$, $d \prec b \prec 1$, $e \prec c \prec 1$, $e \prec b \prec 1$。

引理 6-4.1 在一个布尔格中，$b \wedge \bar{c} = 0$ 当且仅当 $b \preccurlyeq c$。

证明 如果 $b \wedge \bar{c} = 0$，因 $0 \vee c = c$，所以

$$(b \wedge \bar{c}) \vee c = c$$

根据分配性，就有

$$(b \vee c) \wedge (\bar{c} \vee c) = c$$

即 $$(b \vee c) \wedge 1 = c$$

所以 $$b \vee c = c$$

又因 $$b \preccurlyeq b \vee c$$

因此 $$b \preccurlyeq c$$

反之，如果 $b \preccurlyeq c$，则 $$b \wedge \bar{c} \preccurlyeq c \wedge \bar{c}$$

即 $$b\wedge\bar{c}\preccurlyeq 0$$

因此 $$b\wedge\bar{c}=0$$ □

引理 6-4.2 设 $\langle A, \vee, \wedge, {}^{-}\rangle$ 是一个有限布尔代数，若 b 是 A 中任意非零元素，$a_1, a_2, \cdots, a_k$ 是 A 中满足 $a_j\preccurlyeq b$ 的所有原子 $(j=1, 2, \cdots, k)$，则

$$b=a_1\vee a_2\vee\cdots\vee a_k$$

证明 记 $a_1\vee a_2\vee\cdots\vee a_k=c$，因为 $a_j\preccurlyeq b$ $(j=1, 2, \cdots, k)$，所以 $c\preccurlyeq b$。

进一步证明 $b\preccurlyeq c$。由引理 6-4.1 可知，只要设法证明 $b\wedge\bar{c}=0$ 就可以了。为此，我们用反证法。

设 $b\wedge\bar{c}\neq 0$，于是必有一个原子 a，使得 $a\preccurlyeq b\wedge\bar{c}$。

又因 $$b\wedge\bar{c}\preccurlyeq b \quad 和 \quad b\wedge\bar{c}\preccurlyeq\bar{c},$$

所以，由传递性可得

$$a\preccurlyeq b \quad 和 \quad a\preccurlyeq\bar{c}$$

因为 a 是原子，且满足 $a\preccurlyeq b$，所以 a 必是原子 $a_1, a_2, \cdots, a_k$ 中的一个，因此

$$a\preccurlyeq c$$

而由 $a\preccurlyeq\bar{c}$ 和 $a\preccurlyeq c$，便可得

$$a\preccurlyeq c\wedge\bar{c} \quad 即 \quad a\preccurlyeq 0$$

这就与 a 是原子相矛盾。因此，只能有 $b\wedge\bar{c}=0$。

最后，由 $c\preccurlyeq b$ 和 $b\preccurlyeq c$，便得

$$b=c$$

即 $$b=a_1\vee a_2\vee\cdots\vee a_k$$ □

引理 6-4.3 设 $\langle A, \vee, \wedge, {}^{-}\rangle$ 是一个有限布尔代数，$b\in A$，且 $b\neq 0$，$a_1, a_2, \cdots, a_k$ 是满足 $a_i\preccurlyeq b$ $(i=1, 2, \cdots, k)$ 的 A 中的所有原子，则 $b=a_1\vee a_2\vee\cdots\vee a_k$ 是将 b 表示为原子的并的唯一形式。

证明 设有另一种表示式为 $b=a_{j1}\vee a_{j2}\vee\cdots\vee a_{jt}$，其中 $a_{j1}, a_{j2}, \cdots, a_{jt}$ 是 A 中的原子。

因为 b 是 $a_{j1}, a_{j2}, \cdots, a_{jt}$ 的最小上界，所以必有 $a_{j1}\preccurlyeq b$,

$a_{j2} \preccurlyeq b$, $\cdots$, $a_{jt} \preccurlyeq b$。而 $a_1, a_2, \cdots, a_k$ 是 A 中所有满足

$$a_i \preccurlyeq b \quad (i=1, 2, \cdots, k)$$

的不同原子。

所以必有 $$t \leqslant k$$

如果 $t<k$，那么在 $a_1, a_2, \cdots, a_k$ 中必有 a_{j0} 且

$$a_{j0} \neq a_{jl} \quad (1 \leqslant l \leqslant t),$$

于是，由

$$a_{j0} \wedge (a_{j1} \vee a_{j2} \vee \cdots \vee a_{jt}) = a_{j0} \wedge (a_1 \vee a_2 \vee \cdots \vee a_k)$$

便得

$$\begin{aligned}&(a_{j0} \wedge a_{j1}) \vee (a_{j0} \wedge a_{j2}) \vee \cdots \vee (a_{j0} \wedge a_{jt}) \\ =&(a_{j0} \wedge a_1) \vee (a_{j0} \wedge a_2) \vee \cdots \vee \\ &(a_{j0} \wedge a_{j0}) \vee \cdots \vee (a_{j0} \wedge a_k)\end{aligned}$$

这就导致 $0=a_{j0}$ 的矛盾。

所以，只能有 $t=k$ □

引理 6-4.4 在一个布尔格 $\langle A, \preccurlyeq \rangle$ 中，对 A 中的任意一个原子 a 和另一个非零元素 b，$a \preccurlyeq b$ 和 $a \preccurlyeq \bar{b}$ 两式中有且仅有一式成立。

证明　由 $a \preccurlyeq b$ 和 $a \preccurlyeq \bar{b}$，就有 $a \preccurlyeq b \wedge \bar{b} = 0$，这就与 a 是原子相矛盾。所以，两式不可能同时成立。

因为 $a \wedge b \preccurlyeq a$，而 a 是原子，所以只可能有 $a \wedge b = 0$ 或者

$$a \wedge b = a。$$

如果 $a \wedge b = 0$，即 $a \wedge \overline{(\bar{b})} = 0$，于是由引理 6-4.1 便得 $a \preccurlyeq \bar{b}$；如果 $a \wedge b = a$，由定理 6-1.6 便得 $a \preccurlyeq b$。 □

定理 6-4.3(Stone 表示定理)　设 $\langle A, \vee, \wedge, \bar{\ } \rangle$ 是由有限布尔格 $\langle A, \preccurlyeq \rangle$ 所诱导的一个有限布尔代数，S 是布尔格 $\langle A, \preccurlyeq \rangle$ 中的所有原子的集合，则 $\langle A, \vee, \wedge, \bar{\ } \rangle$ 和 $\langle \mathscr{P}(S), \cup, \cap, \sim \rangle$ 同构。

证明　前已证明，对于任何一个非零元素 $a \in A$，必有 a 的一种唯一表示形式

$$a = a_1 \vee a_2 \vee \cdots \vee a_k$$

其中 $a_i(i=1, 2, \cdots, k)$ 是所有满足条件 $a_i \preccurlyeq a$ 的原子的全体。如果记 $S_1=\{a_1, a_2, \cdots, a_k\}$，并作映射

$$f(a)=S_1$$

那么，这个映射 f 是一个从 A 到 $\mathscr{P}(S)$ 的一个双射，这是因为

(1) 特别地，对于 $0\in A$，规定 $f(0)=\emptyset$。

(2) 如果 $S_1=\{a_1, a_2, \cdots, a_k\}\in\mathscr{P}(S)$，而有 $a, b\in A$，使得 $f(a)=f(b)=S_1$，则 $a=a_1\vee a_2\vee\cdots\vee a_k=b$，所以 f 是从 A 到 $\mathscr{P}(S)$ 的入射。

(3) 对于任一个 $S_1\in\mathscr{P}(S)$，若 $S_1=\{a_1, a_2, \cdots, a_k\}$，则由于运算 $\vee$ 的封闭性，所以

$$a_1\vee a_2\vee\cdots\vee a_k=a\in A$$

这就说明 $\mathscr{P}(S)$ 中任一元素，必是 A 中某个元素的象，所以 f 是从 A 到 $\mathscr{P}(S)$ 的满射。

进一步证明 $\langle A, \vee, \wedge, \neg\rangle$ 和 $\langle\mathscr{P}(S), \cup, \cap, \sim\rangle$ 是同构的。这就要求证明：

若 $a, b\in A$，$f(a)=S_1$，$f(b)=S_2$，$S_1, S_2\in\mathscr{P}(S)$ 则

1．$f(a\wedge b)=f(a)\cap f(b)$

2．$f(a\vee b)=f(a)\cup f(b)$

3．$f(\bar{a})=\widetilde{f(a)}$

现分别证明如下：

1．设 $f(a\wedge b)=S_3$，若 $x\in S_3$，则 x 必是满足 $x\preccurlyeq a\wedge b$ 的原子，因为 $a\wedge b\preccurlyeq a$ 和 $a\wedge b\preccurlyeq b$，所以 $x\preccurlyeq a$ 且 $x\preccurlyeq b$，可推得 $x\in S_1$ 且 $x\in S_2$，即 $x\in S_1\cap S_2$，这就证明了 $S_3\sqsubseteq S_1\cap S_2$；

反之，若 $x\in S_1\cap S_2$，则 $x\in S_1$ 且 $x\in S_2$，所以 x 是满足 $x\preccurlyeq a$ 和 $x\preccurlyeq b$ 的原子，由此可推得 x 是满足 $x\preccurlyeq a\wedge b$ 的原子，所以 $x\in S_3$，这就证明了 $S_1\cap S_2\sqsubseteq S_3$。

综上所述，就有 $S_3=S_1\cap S_2$，即

$$f(a\wedge b)=f(a)\cap f(b)$$

2．设 $f(a\vee b)=S_3$，若 $x\in S_3$，则 x 是满足 $x\preccurlyeq a\vee b$ 的原子，

那么必有 $x \preccurlyeq a$ 或 $x \preccurlyeq b$, 这是因为:

若 $x \not\preccurlyeq a$ 且 $x \not\preccurlyeq b$, 则由引理 6-4.4 可知必有 $x \preccurlyeq \bar{a}$ 且 $x \preccurlyeq \bar{b}$, 所以, $x \preccurlyeq \bar{a} \wedge \bar{b} = \overline{a \vee b}$。再由条件 $x \preccurlyeq a \vee b$, 便得

$$x \preccurlyeq (a \vee b) \wedge (\overline{a \vee b}) = 0,$$

这与 x 是原子相矛盾。

因此,若 $x \preccurlyeq a$ 则 $x \in S_1$ 或者若 $x \preccurlyeq b$ 则 $x \in S_2$, 所以

$$x \in S_1 \cup S_2$$

这就证明了 $S_3 \subseteq S_1 \cup S_2$。

反之,若 $x \in S_1 \cup S_2$, 则 $x \in S_1$ 或 $x \in S_2$, 如果 $x \in S_1$ 则

$$x \preccurlyeq a \preccurlyeq a \vee b$$

所以 $x \in S_3$。同理,如果 $x \in S_2$则可推得 $x \in S_3$, 可见

$$S_1 \cup S_2 \subseteq S_3$$

因此, $S_3 = S_1 \cup S_2$ 即 $f(a \vee b) = f(a) \vee f(b)$。

3. 最后证明 $f(\bar{a}) = \widetilde{f(a)}$。将 S 看作全集, 令 $f(a) = S_1$, 则 $\widetilde{f(a)} = S - S_1 = S - f(a)$, 可以证明 $x \in f(\bar{a})$ 当且仅当 $x \not\preccurlyeq a$, 这是因为,如果 $x \in f(\bar{a})$, 必有 $x \preccurlyeq \bar{a}$,那么由引理 6-4.4, 必有 $x \not\preccurlyeq a$,反之, 如果原子 x 满足 $x \not\preccurlyeq a$, 则必有 $x \preccurlyeq \bar{a}$, 所以 $x \in f(\bar{a})$。

还可以证明,对于原子 x, $x \not\preccurlyeq a$ 当且仅当 $x \notin f(a)$,这是因为,若 $x \not\preccurlyeq a$ 而 $x \in f(a)$ 将导致 $x \preccurlyeq a$ 的矛盾,所以 $x \notin f(a)$。反之,若 $x \notin f(a)$而 $x \preccurlyeq a$ 也将导致 $x \in f(a)$的矛盾,所以 $x \not\preccurlyeq a$。

另外,容易证明, $x \notin f(a)$当且仅当 $x \in \widetilde{f(a)}$, 所以, 对于原子 x, $x \in f(\bar{a})$当且仅当 $x \in \widetilde{f(a)}$,因此, $f(\bar{a}) = \widetilde{f(a)}$。

这就证明了 $\langle A, \vee, \wedge, \bar{\ } \rangle$ 和 $\langle \mathscr{P}(S), \cup, \cap, \sim \rangle$ 是同构的,其中 S 是布尔格 $\langle A, \preccurlyeq \rangle$ 中所有原子所组成的集合。 □

由定理 6-4.3 可以有以下的推论。

推论 6-4.1 有限布尔格的元素个数必定等于 2^n, 其中 n 是该布尔格中所有原子的个数。

推论 6-4.2 任何一个具有 2^n 个元素的有限布尔代数都是同构的。

6-4 习题

(1) 证明在布尔代数中，有

$$a \vee (\bar{a} \wedge b) = a \vee b$$

$$a \wedge (\bar{a} \vee b) = a \wedge b$$

(2) 设 $\langle S, \vee, \wedge, ^{-} \rangle$ 是一个布尔代数，$x, y \in S$，证明 $x \leqslant y$ 当且仅当 $\bar{y} \leqslant \bar{x}$。

(3) 设 $\langle A, \vee, \wedge, ^{-} \rangle$ 是一个布尔代数，如果在 A 上定义二元运算 $\oplus$ 为：

$$a \oplus b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$$

证明 $\langle A, \oplus \rangle$ 是一个阿贝尔群。

(4) 设 $\langle A, \vee, \wedge, ^{-} \rangle$ 是一个布尔代数，如果在 A 上定义二元运算 $+$，$\cdot$ 为：

$$a + b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$$

$$a \cdot b = a \wedge b$$

证明 $\langle A, +, \cdot \rangle$ 是以 1 为幺元的环。

(5) 对于题(4)中的二元运算 $+$ 和 $\cdot$，证明

a) $(a+b)+b=a$

b) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

c) $a+a=0$

d) $a+0=a$

e) $a+1=\bar{a}$

(6) 设 $K=\{1, 2, 5, 10, 11, 22, 55, 110\}$ 是 110 的所有整因子的集合，证明：具有全上界 110 和全下界 1 的代数系统 $\langle K, \text{LCM}, \text{GCD}, ' \rangle$ 是一个布尔代数，这里，对于任意的 $x \in K$，$x' = 110/x$。

(7) 设 $\langle K, \vee, \wedge, ' \rangle$ 和 $\langle L, \cup, \cap, ^{-} \rangle$ 是两个布尔代数，并设 f 是从 K 到 L 的同态，即对于任意的 $x, y \in K$，有

$f(x \wedge y) = f(x) \cap f(y)$，　$f(x \vee y) = f(x) \cup f(y)$，　$f(x') = \overline{f(x)}$

试证明：

$$f(0_k) = 0_l$$

$$f(1_k) = 1_l$$

这里，0_k，0_l 和 1_k，1_l 分别是相应的布尔代数中的全下界和全上界。

(8) 设 12 和 24 的整因子集合分别为 $K_1=\{1, 2, 3, 4, 6, 12\}$ 和 $K_2=\{1, 2, 3, 4, 6, 8, 12, 24\}$，试问 $\langle K_1, \text{LCM}, \text{GCD}, ' \rangle$ 和 $\langle K_2, \text{LCM}, \text{GCD}, ' \rangle$ 是布尔代数吗？

(9) 设 $a, b_1, b_2, \cdots, b_r$ 都是布尔代数 $\langle A, \vee, \wedge, ^- \rangle$ 的原子，那么，$a \leqslant (b_1 \vee b_2 \vee \cdots \vee b_r)$ 当且仅当存在着 $i(1 \leqslant i \leqslant r)$ 使得 $a = b_i$。

(10) 设 $b_1, b_2, \cdots, b_r$ 是有限布尔代数 $\langle A, \vee, \wedge, ^- \rangle$ 中的所有原子，那么 $y=0$ 当且仅当对每一个 i 都有 $y \wedge b_i = 0$，这里，$1 \leqslant i \leqslant r$。

6-5 布尔表达式

设 $\langle A, \vee, \wedge, ^- \rangle$ 是一个布尔代数，现考虑一个从 A^n 到 A 的函数。

例 1 设 $A=\{0, 1\}$，那么表 6-5.1 表示了一个从 A^3 到 A 的函数 f；设 $B=\{0, 1, 2, 3\}$，那么表 6-5.2 表示了一个从 B^2 到 B 的函数 g。

以上这种表示函数的方法通常称为列表法。

下面，我们试图用别的方法来描述函数，使之具有紧凑的形式。

定义 6-5.1 设 $\langle A, \vee, \wedge, ^- \rangle$ 是一个布尔代数，并在这个布尔代数上定义布尔表达式如下：

1. A 中任何元素是一个布尔表达式。
2. 任何变元是一个布尔表达式。
3. 如果 e_1 和 e_2 是布尔表达式，那么，$\bar{e}_1$，$(e_1 \vee e_2)$ 和 $(e_1 \wedge e_2)$ 也都是布尔表达式。

表 6-5.1

	f
⟨0, 0, 0⟩	0
⟨0, 0, 1⟩	0
⟨0, 1, 0⟩	1
⟨0, 1, 1⟩	0
⟨1, 0, 0⟩	1
⟨1, 0, 1⟩	1
⟨1, 1, 0⟩	0
⟨1, 1, 1⟩	1

表 6-5.2

	g
$\langle 0, 0\rangle$	1
$\langle 0, 1\rangle$	0
$\langle 0, 2\rangle$	0
$\langle 0, 3\rangle$	3
$\langle 1, 0\rangle$	1
$\langle 1, 1\rangle$	1
$\langle 1, 2\rangle$	0
$\langle 1, 3\rangle$	3
$\langle 2, 0\rangle$	2
$\langle 2, 1\rangle$	0
$\langle 2, 2\rangle$	1
$\langle 2, 3\rangle$	1
$\langle 3, 0\rangle$	3
$\langle 3, 1\rangle$	0
$\langle 3, 2\rangle$	2
$\langle 3, 3\rangle$	2

4. 只有通过有限次运用规则 2 和 3 所构造的符号串是布尔表达式。

例 2 设 $\langle\{0, 1, 2, 3\}, \vee, \wedge, \bar{\ }\rangle$ 是一个布尔代数，那么，$0\wedge x_1$，$(1\vee\bar{x}_1)\wedge x_2$，$((\overline{2\vee 3})\wedge(\bar{x}_1\vee x_2))\wedge(\overline{x_1\wedge x_3})$ 都是布尔表达式，并且分别称为含有单个变元 x_1 的布尔表达式，含有两个变元 x_1，x_2 的布尔表达式和含有三个变元 x_1，x_2，x_3 的布尔表达式。

定义 6-5.2 一个含有 n 个相异变元的布尔表达式，称为含有 n 元的布尔表达式。记为 $E(x_1, x_2, \cdots, x_n)$，其中 x_1，x_2，$\cdots$，x_n 为变元。

定义 6-5.3 布尔代数 $\langle A, \vee, \wedge, \bar{\ }\rangle$ 上的一个含有 n 元的布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 的值是指：将 A 中的元素作为变元 $x_i(i=1, 2, \cdots, n)$ 的值来代替表达式中相应的变元（即对变元赋值），从而计算出表达式的值。

例 3 设布尔代数 $\langle\{0, 1\}, \vee, \wedge, \bar{\ }\rangle$ 上的布尔表达式为

$$E(x_1, x_2, x_3)=(x_1\vee x_2)\wedge(\bar{x}_1\vee\bar{x}_2)\wedge(\overline{x_2\vee x_3})$$

如果变元的一组赋值为 $x_1=1$, $x_2=0$, $x_3=1$, 那么便可求得

$$E(1, 0, 1)=(1\vee 0)\wedge(\bar{1}\vee\bar{0})\wedge(\overline{0\vee 1})=1\wedge 1\wedge 0=0$$

定义 6-5.4 设布尔代数 $\langle A, \vee, \wedge, \bar{\ }\rangle$ 上两个 n 元的布尔表达式为 $E_1(x_1, x_2, \cdots, x_n)$ 和 $E_2(x_1, x_2, \cdots, x_n)$, 如果对于 n 个变元的任意赋值 $x_i=\tilde{x}_i$, $\tilde{x}_i\in A$ 时均有

$$E_1(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n)=E_2(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n)$$

则称这两个布尔表达式是等价的。记作

$$E_1(x_1, x_2, \cdots, x_n)=E_2(x_1, x_2, \cdots, x_n)$$

例 4　在布尔代数 $\langle\{0, 1\}, \vee, \wedge, \bar{\ }\rangle$ 上的两个布尔表达式

$$E_1(x_1, x_2, x_3)=(x_1\wedge x_2)\vee(x_1\wedge\bar{x}_3)$$

和

$$E_2(x_1, x_2, x_3)=x_1\wedge(x_2\vee\bar{x}_3)$$

容易验证, 它们是等价的。譬如:

$$\begin{cases}E_1(0, 1, 1)=(0\wedge 1)\vee(0\wedge 0)=0\vee 0=0\\ E_2(0, 1, 1)=0\wedge(1\vee 0)=0\wedge 1=0\end{cases}$$

$$\begin{cases}E_1(1, 1, 1)=(1\wedge 1)\vee(1\wedge 0)=1\vee 0=1\\ E_2(1, 1, 1)=1\wedge(1\vee 0)=1\wedge 1=1\end{cases}$$

等等。

事实上, 由于布尔代数是有补分配格, 所以当我们对布尔表达式赋值后, 表达式中运算 $\vee$ 对于运算 $\wedge$ 是可分配的, 运算 $\wedge$ 对于运算 $\vee$ 也是可分配的。因此, 如果将布尔表达式中的变元看作是已经赋值的, 那么, 上例中的 E_1 和 E_2 的等价性可以直接写为

$$\begin{aligned}E_2(x_1, x_2, x_3)&=x_1\wedge(x_2\vee\bar{x}_3)=(x_1\wedge x_2)\vee(x_1\wedge\bar{x}_3)\\&=E_1(x_1, x_2, x_3)\end{aligned}$$

对于布尔代数 $\langle A, \vee, \wedge, \bar{\ }\rangle$ 上的任何一个布尔表达式, $E(x_1, x_2, \cdots, x_n)$。由于运算 $\vee$, $\wedge$, $\bar{\ }$ 在 A 上的封闭性, 所以对于任何一个有序 n 元组 $\langle x_1, x_2, \cdots, x_n\rangle$, $x_i\in A$, 可以对应着一个表达式 $E(x_1, x_2, \cdots, x_n)$的值, 这个值必属于 A。由此可见, 我们可以说布尔表达式 $E(x_1, x_2, \cdots, x_n)$确定了一个由 A^n 到 A 的函数。

容易验证, 在布尔代数 $\langle\{0, 1\}, \vee, \wedge, \bar{\ }\rangle$ 上的布尔表达式

$$E(x_1, x_2, x_3)=(x_1 \wedge x_2 \wedge \bar{x}_3) \vee (x_1 \wedge \bar{x}_2) \vee (x_1 \wedge x_2)$$

定义了表 6-5.1 中的从 $\{0, 1\}^3$ 到 $\{0, 1\}$ 的函数。

然而，是否任意一个从 A^n 到 A 的函数都一定能列出一个在 $\langle A, \vee, \wedge, \bar{}\ \rangle$ 上的布尔表达式呢？这个问题的回答将是否定的。

定义 6-5.5 设 $\langle A, \vee, \wedge, \bar{}\ \rangle$ 是一个布尔代数，一个从 A^n 到 A 的函数，如果它能够用 $\langle A, \vee, \wedge, \bar{}\ \rangle$ 上的 n 元布尔表达式来表示，那么，这个函数就称为布尔函数。

定理 6-5.1 对于两个元素的布尔代数 $\langle\{0, 1\}, \vee, \wedge, \bar{}\ \rangle$，任何一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数都是布尔函数。

证明　含有 n 个变元 $x_1, x_2, \cdots, x_n$ 的布尔表达式，如果它有形式 $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$，其中 $\tilde{x}_i$ 是 x_i 或 $\bar{x}_i$ 中的任一个，则我们称这个布尔表达式为小项。一个在 $\langle\{0, 1\}, \wedge, \vee, \bar{}\ \rangle$ 上的布尔表达式，如果它能表示成小项的并，则我们就称这个布尔表达式为析取范式。对于一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数，先用那些使函数值为 1 的有序 n 元组分别构造小项 $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$，其中

$$\tilde{x}_i=\begin{cases} x_i, & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 1 \\ \bar{x}_i, & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 0 \end{cases}$$

然后，再由这些小项所组成析取范式，它就是原来函数所对应的布尔表达式。 □

例 5　讨论表 6-5.3 所给的函数 f 的析取范式和合取范式。

因为函数值为 1 所对应的有序三元组分别为 $\langle 0, 0, 0\rangle$，$\langle 0, 1, 0\rangle$ 和 $\langle 1, 1, 1\rangle$，于是可分别构造小项为 $\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3$，$\bar{x}_1 \wedge x_2 \wedge \bar{x}_3$ 和 $x_1 \wedge x_2 \wedge x_3$。因此，函数 f 所对应的析取范式为

$$(\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3) \vee (\bar{x}_1 \wedge x_2 \wedge \bar{x}_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

它是一个含有三个小项的析取范式的布尔表达式。

类似地，含有 n 个变元 $x_1, x_2, \cdots, x_n$ 的布尔表达式，如果它有形式 $\tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$，其中 $\tilde{x}_i$ 是 x_i 或 $\bar{x}_i$ 中的任一个，则我们称这个布尔表达式为大项。一个在 $\langle\{0, 1\}, \vee, \wedge, \bar{}\ \rangle$ 上的布尔表达式，如果它能表示成大项的交，则我们就称这个布尔表达式为合

表 6-5.3

	f
$\langle 0,\ 0,\ 0\rangle$	1
$\langle 0,\ 0,\ 1\rangle$	0
$\langle 0,\ 1,\ 0\rangle$	1
$\langle 0,\ 1,\ 1\rangle$	0
$\langle 1,\ 0,\ 0\rangle$	0
$\langle 1,\ 0,\ 1\rangle$	0
$\langle 1,\ 1,\ 0\rangle$	0
$\langle 1,\ 1,\ 1\rangle$	1

取范式。那么,对于一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数,我们可以用那些使函数值为 0 的有序 n 元组分别构造大项 $\tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$,其中

$$\tilde{x}_i = \begin{cases} x_i, & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 0 \\ \bar{x}_i, & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 1 \end{cases}$$

那么,由这些大项所组成的合取范式,就是原来函数所对应的布尔表达式。

因此,对于表 6-5.3 中的函数 f,如果用合取范式来表示,就应该是

$$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_3)$$
$$\wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3)$$

它是一个含有五个大项的合取范式。

正因为任何一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数,它的函数值只可能是 1 或 0,因此,总可以用上述方法得到该函数所对应的析取范式、合取范式。

下面,我们将布尔代数 $\langle\{0, 1\}, \vee, \wedge, \bar{\ }\rangle$ 上的布尔表达式的析取范式和合取范式的概念扩充到一般的布尔代数上。假如 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle A, \vee, \wedge, \bar{\ }\rangle$ 上的一个布尔表达式。如果这个布尔表达式能够表示成形如

$$C_{\delta_1\delta_2\cdots\delta_n} \wedge \tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$$

的并,其中 $C_{\delta_1\delta_2\cdots\delta_n}$ 是 A 中的一个元素,$\tilde{x}_i$ 是 x_i 或 $\bar{x}_i$ 中任一个,则

称这种布尔表达式为析取范式。

定理6-5.2 设 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle A, \vee, \wedge, ^- \rangle$ 上的任意一个布尔表达式，则它一定能写成析取范式。

证明 令 $E(x_i=a)=E(x_1, x_2, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n)$，$a\in A$。表达式 $E(x_1, x_2, \cdots, x_n)$ 的长度定义为该表达式中出现的 A 的元素个数、变元的个数以及 $\vee$，$\wedge$，$^-$ 的个数的总和（如果重复出现就要重复计数）。记 $E(x_1, x_2, \cdots, x_n)$ 的长度为 $|E|$。

首先证明：对于任何 x_i，必有

$$E(x_1, x_2, \cdots, x_n)=(\bar{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))$$

对 $|E|$ 用归纳证明。

若 $|E|=1$，则 $E=a$ 或 $E=x_j$，如果 $E=a$，则有

$$E(x_i=0)=E(x_i=1)=a$$

所以
$$\begin{aligned}E=a&=(\bar{x}_i\vee x_i)\wedge a=(\bar{x}_i\wedge a)\vee(x_i\wedge a)\\&=(\bar{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

如果 $j=i$，显然有 $E(x_i=0)=0$，$E(x_i=1)=1$，所以

$$\begin{aligned}E=x_j&=(\bar{x}_i\wedge 0)\vee(x_i\wedge 1)\\&=(\bar{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

如果 $j\neq i$，显然有 $E(x_i=0)=E(x_i=1)=x_j$，所以

$$\begin{aligned}E=x_j&=(\bar{x}_i\vee x_i)\wedge x_j=(\bar{x}_i\wedge x_j)\vee(\bar{x}_i\wedge x_j)\\&=(\bar{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

因此，$|E|=1$ 时，$E=(\bar{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))$ 成立。

设 $|E|\leq n$ 时，结论成立。当 $|E|=n+1$ 时，有以下三种情况：

1. 如果 $E=E_1\vee E_2$，则必有 $|E_1|\leq n$，$|E_2|\leq n$，因此由归纳假设，就有

$$E_1=(\bar{x}_i\wedge E_1(x_i=0))\vee(x_i\wedge E_1(x_i=1))$$

$$E_2=(\bar{x}_i\wedge E_2(x_i=0))\vee(x_i\wedge E_2(x_i=1))$$

所以
$$\begin{aligned}E=E_1\vee E_2&=[(\bar{x}_i\wedge E_1(x_i=0))\vee(x_i\wedge E_1(x_i=1))]\\&\quad\vee[(\bar{x}_i\wedge E_2(x_i=0))\vee(x_i\wedge E_2(x_i=1))]\\&=[\bar{x}_i\wedge(E_1(x_i=0)\vee E_2(x_i=0))]\end{aligned}$$

$$\vee [x_i \wedge (E_1(x_i=1) \vee E_2(x_i=1))]$$
$$= (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))$$

2. 如果 $E=E_1 \wedge E_2$, 则必有 $|E_1| \leqq n$, $|E_2| \leqq n$, 同样由归纳假设，就有

$$\begin{aligned}
E = E_1 \wedge E_2 &= [(\bar{x}_i \wedge E_1(x_i=0)) \vee (x_i \wedge E_1(x_i=1))] \\
&\quad \wedge [(\bar{x}_i \wedge E_2(x_i=0)) \vee (x_i \wedge E_2(x_i=1))] \\
&= [(\bar{x}_i \wedge E_1(x_i=0)) \wedge (\bar{x}_i \wedge E_2(x_i=0))] \\
&\quad \vee [(x_i \wedge E_1(x_i=1)) \wedge (\bar{x}_i \wedge E_2(x_i=0))] \\
&\quad \vee [(\bar{x}_i \wedge E_1(x_i=0)) \wedge (x_i \wedge E_2(x_i=1))] \\
&\quad \vee [(x_i \wedge E_1(x_i=1)) \wedge (x_i \wedge E_2(x_i=1))] \\
&= [\bar{x}_i \wedge (E_1(x_i=0) \wedge E_2(x_i=0))] \\
&\quad \vee [x_i \wedge (E_1(x_i=1) \wedge E_2(x_i=1))] \\
&= (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))
\end{aligned}$$

3. 如果 $E=\overline{E}_1$, 则必有 $|E_1|=n$, 由归纳假设，即有

$$\begin{aligned}
E = \overline{E}_1 &= \overline{(\bar{x}_i \wedge E_1(x_i=0)) \vee (x_i \wedge E_1(x_i=1))} \\
&= \overline{(\bar{x}_i \wedge E_1(x_i=0))} \wedge \overline{(x_i \wedge E_1(x_i=1))} \\
&= (x_i \vee \overline{E}_1(x_i=0)) \wedge (\bar{x}_i \vee \overline{E}_1(x_i=1)) \\
&= [(x_i \vee \overline{E}_1(x_i=0)) \wedge \bar{x}_i] \\
&\quad \vee [(x_i \vee \overline{E}_1(x_i=0)) \wedge \overline{E}_1(x_i=1)] \\
&= [(x_i \wedge \bar{x}_i) \vee (\overline{E}_1(x_i=0) \wedge \bar{x}_i)] \\
&\quad \vee [(x_i \wedge \overline{E}_1(x_i=1)) \vee (\overline{E}_1(x_i=0) \wedge \overline{E}_1(x_i=1))] \\
&= (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1)) \\
&\quad \vee [(\bar{x}_i \vee x_i) \wedge (E(x_i=0) \wedge E(x_i=1))] \\
&= (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1)) \\
&\quad \vee (\bar{x}_i \wedge E(x_i=0) \wedge E(x_i=1)) \\
&\quad \vee (x_i \wedge E(x_i=0) \wedge E(x_i=1)) \\
&= [(\bar{x}_i \wedge E(x_i=0)) \wedge (1 \vee E(x_i=1))] \\
&\quad \vee [(x_i \wedge E(x_i=1)) \wedge (1 \vee E(x_i=0))] \\
&= (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))
\end{aligned}$$

由上面证明的结果

$$E(x_1, x_2, \cdots, x_n) = (\bar{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))$$

可得

$$\begin{aligned}
E(x_1, x_2, \cdots, x_n) &= (\bar{x}_1 \wedge E(0, x_2, \cdots, x_n)) \\
&\quad \vee (x_1 \wedge E(1, x_2, \cdots, x_n)) \\
&= \{\bar{x}_1 \wedge [(\bar{x}_2 \wedge E(0, 0, x_3, \cdots, x_n)) \\
&\quad \vee (x_2 \wedge E(0, 1, x_3, \cdots, x_n))]\} \\
&\quad \vee \{x_1 \wedge [(\bar{x}_2 \wedge E(1, 0, x_3, \cdots, x_n)) \\
&\quad \vee (x_2 \wedge E(1, 1, x_3, \cdots, x_n))]\} \\
&= [\bar{x}_1 \wedge \bar{x}_2 \wedge E(0, 0, x_3, \cdots, x_n)] \\
&\quad \vee [\bar{x}_1 \wedge x_2 \wedge E(0, 1, x_3, \cdots, x_n)] \\
&\quad \vee [x_1 \wedge \bar{x}_2 \wedge E(1, 0, x_3, \cdots, x_n)] \\
&\quad \vee [x_1 \wedge x_2 \wedge E(1, 1, x_3, \cdots, x_n)] \\
&= \cdots \\
&= [\bar{x}_1 \wedge \bar{x}_2 \wedge \cdots \wedge \bar{x}_n \wedge E(0, 0, \cdots, 0)] \\
&\quad \vee [\bar{x}_1 \wedge \bar{x}_2 \wedge \cdots \wedge \bar{x}_{n-1} \wedge x_n \\
&\quad \wedge E(0, 0, \cdots, 0, 1)] \\
&\quad \vee \cdots \vee [x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1} \wedge \bar{x}_n \\
&\quad \wedge E(1, 1, \cdots, 1, 0)] \\
&\quad \vee [x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge E(1, 1, \cdots, 1)]
\end{aligned}$$

其中每一个方括号里的布尔表达式可以写成统一形式

$$C_{\delta_1\delta_2\cdots\delta_n} \wedge \tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$$

而 $C_{\delta_1\delta_2\cdots\delta_n} \in A$, $\tilde{x}_i$ 是 x_i 或 $\bar{x}_i$ 中的一个。 □

类似地，我们可以通过证明

$$E(x_1, x_2, \cdots, x_n) = (x_i \vee E(x_i=0)) \wedge (\bar{x}_i \vee E(x_i=1))$$

来证明任何布尔表达式能够写成形如

$$D_{\delta_1\delta_2\cdots\delta_n} \vee \tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$$

的交，其中 $D_{\delta_1\delta_2\cdots\delta_n} \in A$, $\tilde{x}_i$ 表示 x_i 或 $\bar{x}_i$ 中的一个。即表示成合取范式，这里就不再赘述了。

例题 1　表 6-5.2 中所确定的从 B^2 到 B 的函数 g, 其中

$$B=\{0, 1, 2, 3\}$$

证明 g 不是布尔函数。

证明　用反证法。

如果是布尔函数，那么它的布尔表达式必可表示成析取范式为：

$$g(x_1, x_2)=(C_{11}\wedge x_1\wedge x_2)\vee(C_{12}\wedge x_1\wedge \bar{x}_2)$$
$$\vee(C_{21}\wedge \bar{x}_1\wedge x_2)\vee(C_{22}\wedge \bar{x}_1\wedge \bar{x}_2)$$

从表 6-5.2 可知

$$C_{11}=g(1, 1)=1$$
$$C_{12}=g(1, 0)=1$$
$$C_{21}=g(0, 1)=0$$
$$C_{22}=g(0, 0)=1$$

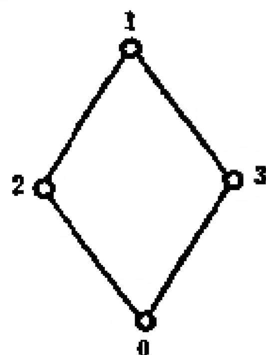


图　6-5.1

所以

$$g(x_1, x_2)=(x_1\wedge x_2)$$
$$\vee(x_1\wedge \bar{x}_2)\vee(\bar{x}_1\wedge \bar{x}_2)$$

对于布尔格 $\langle\{0, 1, 2, 3\}, \preccurlyeq\rangle$ 可用图 6-5.1 的哈斯图来表示。

由图 6-5.1 可知

$$g(3, 3)=(3\wedge 3)\vee(3\wedge 2)\vee(2\wedge 2)$$
$$=3\vee 0\vee 2=1$$

这就与表 6-5.2 中的 $g(3, 3)=2$ 相矛盾，所以表 6-5.2 中的函数不是布尔函数。

作为布尔代数的直接应用，我们可以确认：

命题逻辑可以用布尔代数 $\langle\{F, T\}, \vee, \wedge, ^{-}\rangle$ 来描述，一个原子命题就是一个变元，它的取值为 T 或 F，因此，任一复合命题都可以用代数系统 $\langle\{F, T\}, \vee, \wedge, ^{-}\rangle$ 上的一个布尔函数来表示。

开关代数可以用布尔代数 〈{断开、闭合}，并联，串联，反向〉来描述，一个开关就是一个变元，它的取值为“断开”或“闭合”，因此，任一开关线路都可以用代数系统〈{断开，闭合}，并联，串联，反向〉上的一个布尔函数来表示。

6-5　习题

(1) 设 $E(x_1, x_2, x_3)=(x_1\wedge x_2)\vee(x_2\wedge x_3)\vee(\bar{x}_2\wedge x_3)$ 是布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^{-}\rangle$ 上的一个布尔表达式。试写出 $E(x_1, x_2, x_3)$ 的析取范

式和合取范式。

(2) 设 $E(x_1, x_2, x_3, x_4)=(x_1 \wedge x_2 \wedge \bar{x}_3) \vee (x_1 \wedge \bar{x}_2 \wedge x_4) \vee (x_2 \wedge \bar{x}_3 \wedge \bar{x}_4)$ 是布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^-\rangle$ 上的一个布尔表达式。试写出 $E(x_1, x_2, x_3, x_4)$ 的析取范式和合取范式。

(3) 对于表 6-5.4 中的函数 f，试分别用析取范式和合取范式来表示。

表 **6-5.4**

	f
⟨0, 0, 0⟩	1
⟨0, 0, 1⟩	0
⟨0, 1, 0⟩	1
⟨0, 1, 1⟩	0
⟨1, 0, 0⟩	0
⟨1, 0, 1⟩	1
⟨1, 1, 0⟩	0
⟨1, 1, 1⟩	1

第四篇 图　　论

图论是近年来发展迅速而又应用广泛的一门新兴学科。它最早起源于一些数学游戏的难题研究，如 1736 年欧拉 (L. Euler) 所解决的哥尼斯堡 (Königsberg) 七桥问题，以及在民间广泛流传的一些游戏难题，如迷宫问题，匿门博奕问题，棋盘上马的行走路线问题等。这些古老的难题，当时吸引了很多学者的注意，在这些问题研究的基础上又继续提出了著名的四色猜想，汉密尔顿(环游世界)数学难题。

1847 年，克希霍夫 (Kirchhoff) 用图论分析电路网络，这是图论最早应用于工程科学，以后随着科学的发展，图论在解决运筹学，网络理论，信息论，控制论，博奕论以及计算机科学等各个领域的问题时，显示出越来越大的效果。图论在各种物理学科，工程领域，社会科学和经济问题的广泛应用，使它受到数学和工程界的特别重视。对于这样一门应用广泛的学科，其包含的内容当然是浩瀚如海，我们这里只准备介绍一些基本概念和定理，以及一些典型的应用实例，目的是在今后对计算机有关学科的学习研究时，可以图论的基本知识作为工具。

第七章　图　论

7-1　图的基本概念

现实世界中许多状态是由图形来描述的。一个图是由一些结点和连接两个结点之间的连线所组成，至于连线的长度及结点的

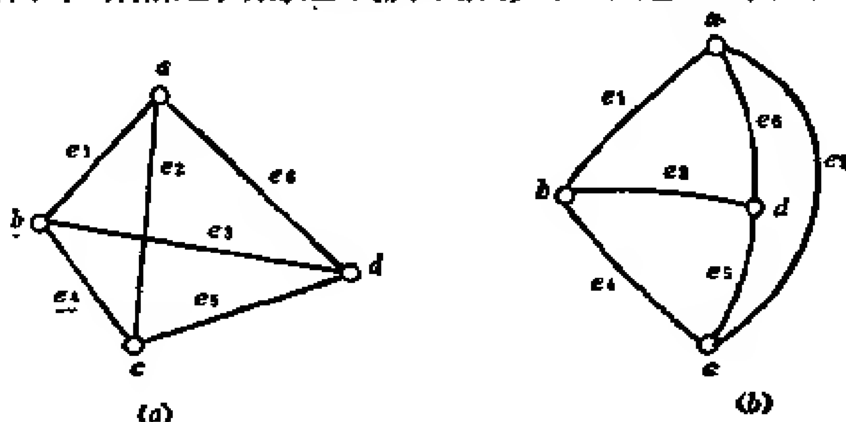


图　7-1.1

位置是无关紧要的。如图 7-1.1(a)和(b)表示了同一个图形。

定义 7-1.1　一个图是一个三元组 $\langle V(G), E(G), \varphi_G\rangle$，其中 $V(G)$是一个非空的结点集合，$E(G)$是边集合，φ_G 是从边集合 E 到结点无序偶(有序偶)集合上的函数。

例 1　　$G=\langle V(G), E(G), \varphi_G\rangle$

其中 $V(G)=\{a, b, c, d\}$，$E(G)=\{e_1, e_2, e_3, e_4, e_5, e_6\}$，$\varphi_G(e_1)=(a, b)$，$\varphi_G(e_2)=(a, c)$，$\varphi_G(e_3)=(b, d)$，$\varphi_G(e_4)=(b, c)$，$\varphi_G(e_5)=(d, c)$，$\varphi_G(e_6)=(a, d)$。

一个图可用一个图形表示，例 1 可表示为图 7-1.1(a)或(b)。

若把图中的边 e_i 看作总是与两个结点关联，那么一个图亦可简记为 $G=\langle V, E\rangle$，其中 V 是非空结点集，E 是连接结点的边集。

若边 e_i 与结点无序偶(v_j, v_k)相关联，则称该边为无向边。

若边 e_i' 与结点有序偶 $\langle v_j, v_k\rangle$ 相关联，则称该边为有向边。

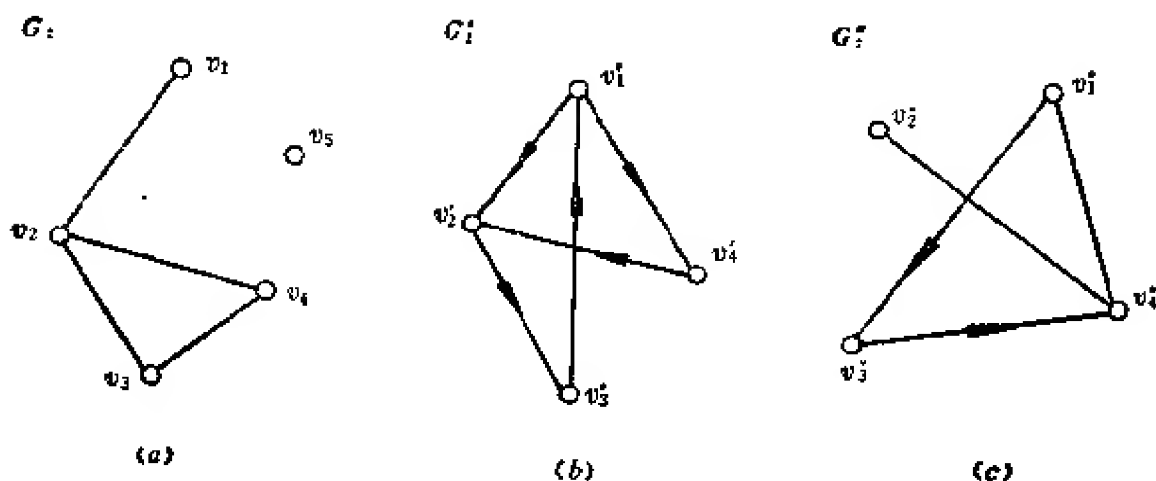


图 7-1.2

其中 v_j 称为 e_i' 的起始结点；v_k 称为 e_i' 的终止结点。

每一条边都是无向边的图称无向图，如图 7-1.2(a)所示。

每一条边都是有向边的图称有向图，如图 7-1.2(b)所示。

如果在图中一些边是有向边，另一些边是无向边，则称这个图是混合图，如图 7-1.2(c)所示。这些图可分别表示为：

$$G=\langle V, E\rangle=\langle\{v_1, v_2, v_3, v_4, v_5\}, \{(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_2, v_4)\}\rangle$$

$$G'=\langle V', E'\rangle=\langle\{v_1', v_2', v_3', v_4'\}, \{\langle v_1', v_2'\rangle, \langle v_2', v_3'\rangle, \langle v_3', v_1'\rangle, \langle v_1', v_4'\rangle, \langle v_4', v_2'\rangle\}\rangle$$

$$G''=\langle V'', E''\rangle=\langle\{v_1'', v_2'', v_3'', v_4''\}, \{(v_1'', v_4''), (v_2'', v_4''), \langle v_1'', v_3''\rangle, \langle v_3'', v_4''\rangle\}\rangle$$

今后我们只讨论有向图和无向图。

在一个图中，若两个结点由一条有向边或一条无向边关联，则这两个结点称为是邻接点。

在一个图中不与任何结点相邻接的结点，称为孤立结点，如图 7-1.2(a)中的结点 v_5。仅由孤立结点组成的图称为零图，仅由一个孤立结点构成的图称为平凡图。

类似于邻接点的概念，关联于同一结点的两条边称为邻接边。关联于同一结点的一条边称为自回路或环。如图 7-1.3 中(c, c)是环。环的方向是没有意义的，它既可作为有向边，也可作无向边。

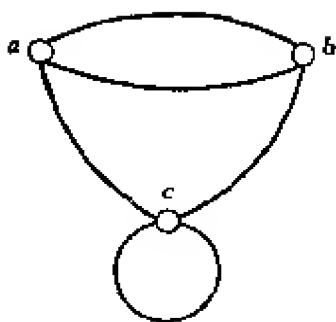


图 7-1.3

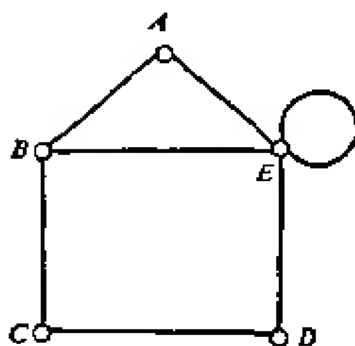


图 7-1.4

定义 7-1.2 在图 $G=\langle V, E\rangle$ 中，与结点 $v(v\in V)$ 关联的边数，称作是该结点的度数，记作 $\deg(v)$。

例如在图 7-1.4 中，结点 A 的度数为 2，结点 B 的度数为 3，我们约定：每个环在其对应结点上度数增加 2。故图 7-1.4 中结点 E 的度数为 5。

此外，我们记 $\Delta(G)=\max\{\deg v \mid v\in V(G)\}$，$\delta(G)=\min\{\deg v \mid v\in V(G)\}$，分别称为 $G=\langle V, E\rangle$ 的最大度和最小度。如图 7-1.4 中 $\Delta(G)=5$，$\delta(G)=2$。

定理 7-1.1 每个图中，结点度数的总和等于边数的两倍。

$$\sum_{v\in V}\deg(v)=2|E|$$

证明 因为每条边必关联两个结点，而一条边给予关联的每个结点的度数为 1。因此在一个图中，结点度数的总和等于边数的两倍。 □

定理 7-1.2 在任何图中，度数为奇数的结点必定是偶数个。

证明 设 V_1 和 V_2 分别是 G 中奇数度数和偶数度数的结点集，则由定理 7-1.1，有

$$\sum_{v\in V_1}\deg(v)+\sum_{v\in V_2}\deg(v)=\sum_{v\in V}\deg(v)=2|E|$$

由于 $\sum_{v\in V_2}\deg(v)$ 是偶数之和，必为偶数，而 $2|E|$ 是偶数，故得 $\sum_{v\in V_1}\deg(v)$ 是偶数，即 $|V_1|$ 是偶数。 □

定义 7-1.3 在有向图中，射入一个结点的边数称为该结点的入度，由一个结点射出的边数称为该结点的出度。结点的出度

与入度之和就是该结点的度数。

定理 7-1.3 在任何有向图中，所有结点的入度之和等于所有结点的出度之和。

证明 因为每一条有向边必对应一个入度和一个出度，若一个结点具有一个入度或出度，则必关联一条有向边，所以，有向图中各结点入度之和等于边数，各结点出度之和也等于边数，因此，任何有向图中，入度之和等于出度之和。 □

在上面所讲图的概念中，一个结点的度数可能大于 1，但是任何一对结点间常常不多于一条边。我们把连接于同一对结点间的多条边称为是平行的。

定义 7-1.4 含有平行边的任何一个图称为多重图。

例如图 7-1.5 所示的均为多重图。在图 7-1.5(a) 中结点 a 和 b 之间有两条平行边，结点 b 和 c 之间有三条平行边，在结点 b 有两个平行的环。结点 a 的度数为 3，结点 c 的度数为 4，结点 b 的度数为 9。在图 7-1.5(b) 中，只有结点 v_1 和 v_2 之间有两条平行边。这是因为该有向图中，$\langle v_1, v_2\rangle$ 与 $\langle v_2, v_1\rangle$ 认为是不同的结点对。

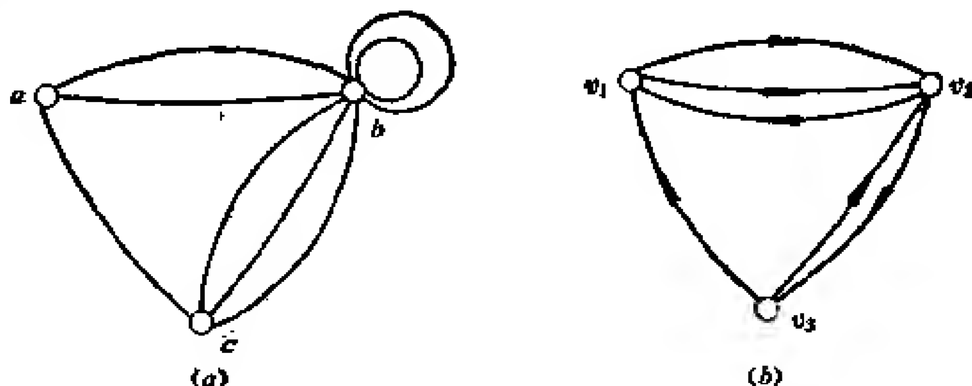


图 7-1.5

今后我们把不含有平行边和环的图称作简单图。

定义 7-1.5 简单图 $G=\langle V, E\rangle$ 中，若每一对结点间都有边相连，则称该图为完全图。

有 n 个结点的无向完全图记作 K_n。

定理 7-1.4 n 个结点的无向完全图 K_n 的边数为 $\frac{1}{2}n(n-1)$。

证明　在 K_n 中，任意两点间都有边相连，n 个结点中任取两点的组合数为：

$$C_n^2=\frac{1}{2}n(n-1)$$

故 K_n 的边数为

$$|E|=\frac{1}{2}n(n-1) \qquad \Box$$

如果在 K_n 中，对每条边任意确定一个方向，就称该图为 n 个结点的有向完全图。显然，它的边数也为 $\frac{1}{2}n(n-1)$。

给定任意一个含有 n 个结点的图 G，总可以把它补成一个具有同样结点的完全图，方法是把那些没有联上的边添加上去。

定义 7-1.6　给定一个图 G，由 G 中所有结点和所有能使 G 成为完全图的添加边组成的图，称为 G 的相对于完全图的补图，或简称为 G 的补图，记作 $\overline{G}$。

如图 7-1.6 中 (a) 和 (b) 互为补图。



图　7-1.6

定义 7-1.7　设图 $G=\langle V, E\rangle$，如果有图 $G'=\langle V', E'\rangle$，且

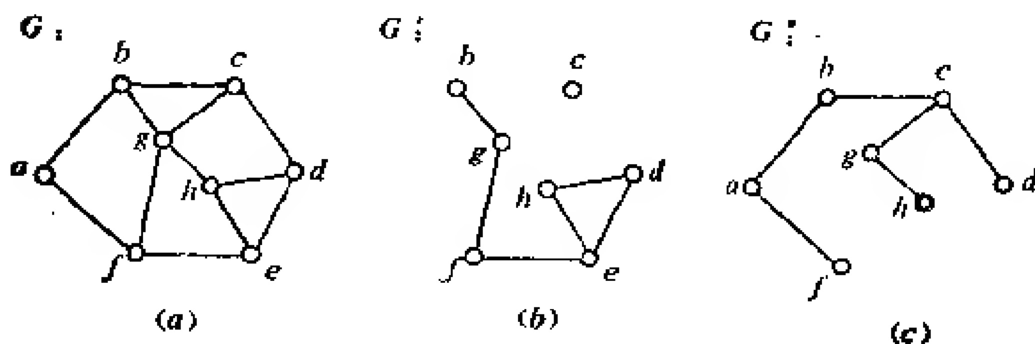


图　7-1.7

$E' \subseteq E$, $V' \subseteq V$, 则称 G' 为 G 的子图。

如图 7-1.7 中 (b) 和 (c) 都是 (a) 的子图。

如果 G 的子图包含 G 的所有结点，则称该子图为 G 的生成子图。如图 7-1.8 中 G' 和 G'' 都是 G 的生成子图。

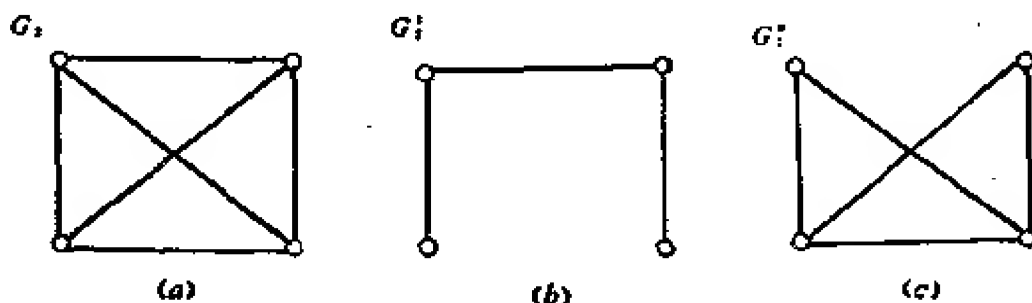


图 7-1.8

定义 7-1.8 设 $G'=\langle V', E'\rangle$ 是图 $G=\langle V, E\rangle$ 的子图，若给定另外一个图 $G''=\langle V'', E''\rangle$ 使得 $E''=E-E'$，且 V'' 中仅包含 E'' 的边所关联的结点。则称 G'' 是子图 G' 的相对于图 G 的补图。

例如图 7-1.7 中图 (c) 是图 (b) 相对于图 (a) 的补图。而图 (b) 不是图 (c) 相对于图 (a) 的补图，因为图 (b) 中有结点 c。

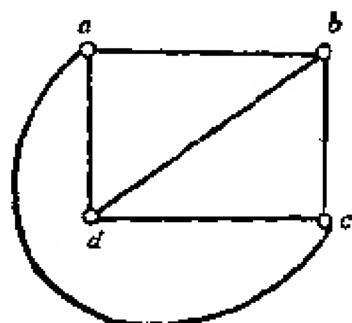
在上面一些图的基本概念中，一个图由一个图形表示，由于图形的结点位置和连线长度都可任意选择，故一个图的图形表示并不是唯一的。下面我们讨论图的同构的概念。

定义 7-1.9 设图 $G=\langle V, E\rangle$ 及图 $G'=\langle V', E'\rangle$，如果存在一一对应的映射 $g: v_i \rightarrow v_i'$ 且 $e=(v_i, v_j)$（或 $\langle v_i, v_j\rangle$）是 G 的一条边，当且仅当 $e'=(g(v_i), g(v_j))$（或 $\langle g(v_i), g(v_j)\rangle$）是 G' 的一条边，则称 G 与 G' 同构，记作 $G \simeq G'$。

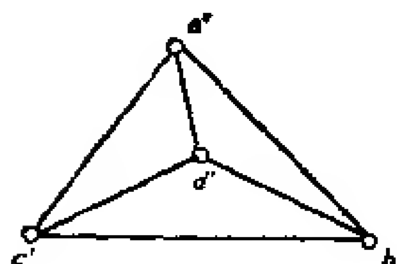
从这个定义可以看到，若 G 与 G' 同构，它的充要条件是：两个图的结点和边分别存在着一一对应，且保持关联关系，例如图 7-1.9 中，(a) 与 (b) 是同构的，(c) 与 (d) 也是同构的。

从图 7-1.9 的 (c) 与 (d) 中可以看到此两图在结点间存在着一一对应映射 g: $g(a)=u_3$, $g(b)=u_1$, $g(c)=u_4$, $g(d)=u_2$，且有：$\langle a, c\rangle$, $\langle a, b\rangle$, $\langle b, d\rangle$, $\langle c, d\rangle$ 分别与 $\langle u_3, u_4\rangle$, $\langle u_3, u_1\rangle$, $\langle u_1, u_2\rangle$,

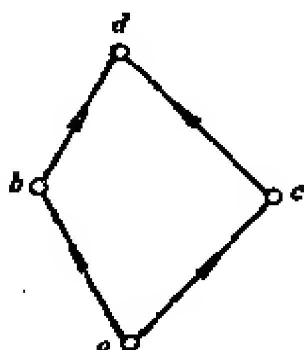
$\langle u_4, u_2\rangle$ 一一对应。



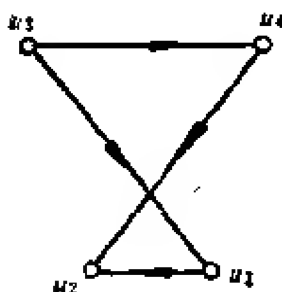
(a)



(b)



(c)



(d)

图 7-1.9

分析本例还可以知道，此两图的结点度数也分别对应相等，如表 7-1.1 所示。

表 7-1.1

度名 \ 数目	结点			
	a	b	c	d
出度	2	1	1	0
入度	0	1	1	2

度名 \ 数目	结点			
	u_1	u_2	u_3	u_4
出度	1	0	2	1
入度	1	2	0	1

综上所述，可以得到两图同构的一些必要条件：

1．结点数目相同；

2．边数相等；

3．度数相同的结点数目相等。

需要指出的是这几个条件不是两个图同构的充分条件，例如图 7-1.10 中(*a*)和(*b*)满足上述三个条件，但此两个图并不同构。

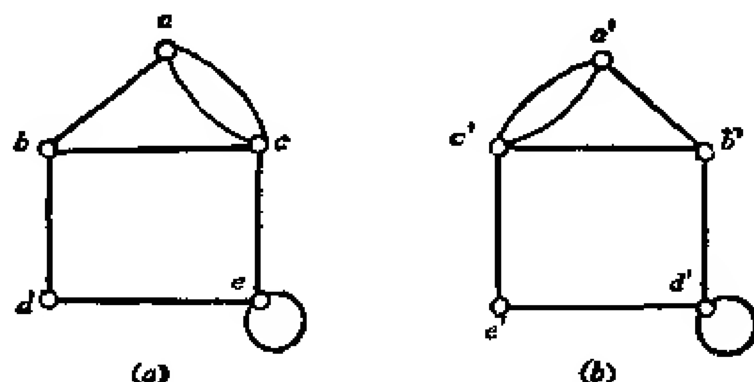


图 7-1.10

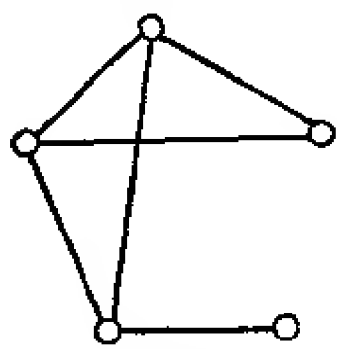
7-1 习题

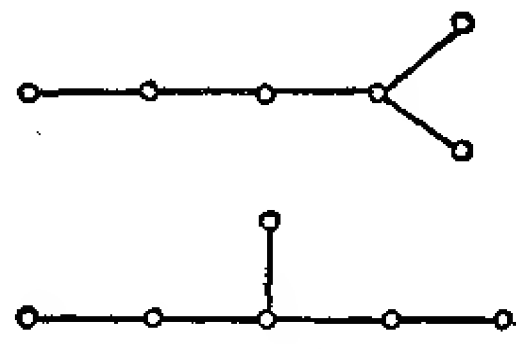
(1) 证明在任何有向完全图中，所有结点入度的平方之和等于所有结点的出度平方之和。

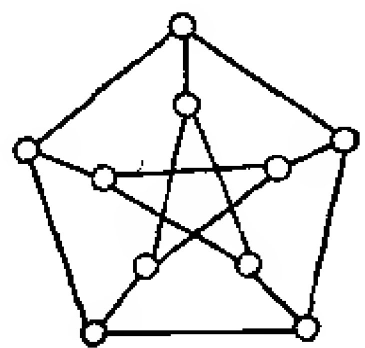
(2) 写出图 7-1.11 相对于完全图的补图。

(3) 证明图 7-1.12 中两个图不同构。

(4) 证明图 7-1.13 中两个图是同构的。


图 7-1.11


图 7-1.12



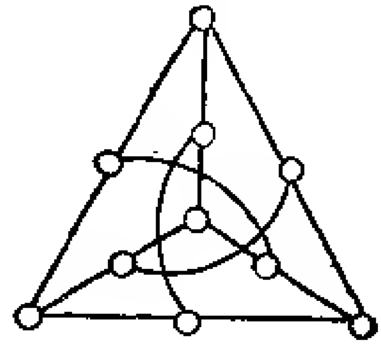


图 7-1.13

(5) 一个图如果同构于它的补图，则该图称为自补图。

a) 试给出一个五个结点的自补图。

b) 是否有三个结点或六个结点的自补图。

c) 一个图是自补图，其对应的完全图的边数必为偶数。

(6) 证明简单图的最大度小于结点数。

7-2 路与回路

在现实世界中，常常要考虑这样的问题：如何从一个图 G 中的给定结点出发，沿着一些边连续移动而到达另一指定结点，这种依次由点和边组成的序列，就形成了路的概念。

定义 7-2.1 给定图 $G=\langle V, E\rangle$，设 $v_0, v_1, \cdots, v_n \in V$，$e_1, e_2, \cdots, e_n \in E$，其中 e_i 是关联于结点 v_{i-1}，v_i 的边，交替序列 $v_0 e_1 v_1 e_2 \cdots e_n v_n$ 称为联结 v_0 到 v_n 的路。

v_0 和 v_n 分别称作路的起点和终点，边的数目 n 称作路的长度。当 $v_0=v_n$ 时，这条路称作回路。

若一条路中所有的边 $e_1, e_2, \cdots, e_n$ 均不相同，称作迹。若一条路中所有的结点 $v_0, v_1, \cdots, v_n$ 均不相同，则称作通路。闭的通路，即除 $v_0=v_n$ 外，其余的结点均不相同的路，就称作圈。

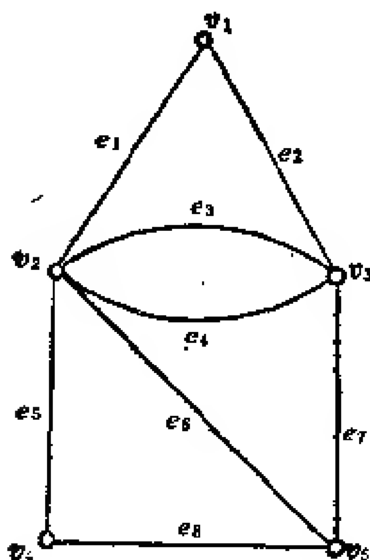


图 7-2.1

例如在图 7-2.1 中有：

路：$v_1e_2v_3e_3v_2e_3v_3e_4v_2e_6v_5e_7v_3$

迹：$v_5e_8v_4e_5v_2e_6v_5e_7v_3e_4v_2$

通路：$v_4e_8v_5e_6v_2e_1v_1e_2v_3$

圈：$v_2e_1v_1e_2v_3e_7v_5e_6v_2$

在简单图中一条路 $v_0 e_1 v_1 e_2 \cdots e_n v_n$，由它的结点序列 $v_0 v_1 \cdots v_n$ 确定，所以简单图的路，可由其结点序列表示。在有向图中，结点数大于一的一条路亦可由边序列 $e_1 e_2 \cdots e_n$ 表示。

定理 7-2.1 在一个具有 n 个结点的图中，如果从结点 v_j 到结点 v_k 存在一条路，则从结点 v_j 到结点 v_k 必存在一条不多于 $n-1$ 条边的路。

证明 如果从结点 v_j 到结点 v_k 存在一条路，该路上的结点序列是 $v_j \cdots v_i \cdots v_k$，如果在这条路中有 l 条边，则序列中必有 $l+1$ 个结点，若 $l>n-1$，则必有结点 v_s，它在序列中不止一次出现，即必有结点序列 $v_j \cdots v_s \cdots v_s \cdots v_k$，在路中去掉从 v_s 到 v_s 的这些边，仍是 v_j 到 v_k 的一条路，但此路比原来的路边数要少，如此重复进行下去，必可得到一条从 v_j 到 v_k 的不多于 $n-1$ 条边的路。 □

推论 在一个具有 n 个结点的图中，若从结点 v_j 到 v_k 存在一条路，则必存在一条从 v_j 到 v_k 而边数小于 n 的通路。

定义 7-2.2 在无向图 G 中，结点 u 和 v 之间若存在一条路，则称结点 u 和结点 v 是连通的。

不难证明，结点之间连通性是结点集 V 上的等价关系，因此对应这个等价关系，必可对结点集 V 作出一个划分，把 V 分成非空子集 $V_1, V_2, \cdots, V_m$，使得两个结点 v_j 和 v_k 是连通的，当且仅当它们属于同一个 V_i。我们把子图 $G(V_1), G(V_2), \cdots, G(V_m)$ 称为图 G 的连通分支(图)，今后我们把图 G 的连通分支数记作 $W(G)$。

定义 7-2.3 若图 G 只有一个连通分支，则称 G 是连通图。

显然在连通图中，任意两个结点之间必是连通的。例如图 7-2.2 中 (a) 是连通图，(b) 是具有三个连通分支的非连通图。

对于连通图，常常由于删除了图中的点或边，而影响了图的连通性，所谓在图中删除结点 v，即是把 v 以及与 v 关联的边都删去，例如，在图 7-2.3 (a) 中删除 v_1，即由图 (a) 变为图 (b)。所谓在

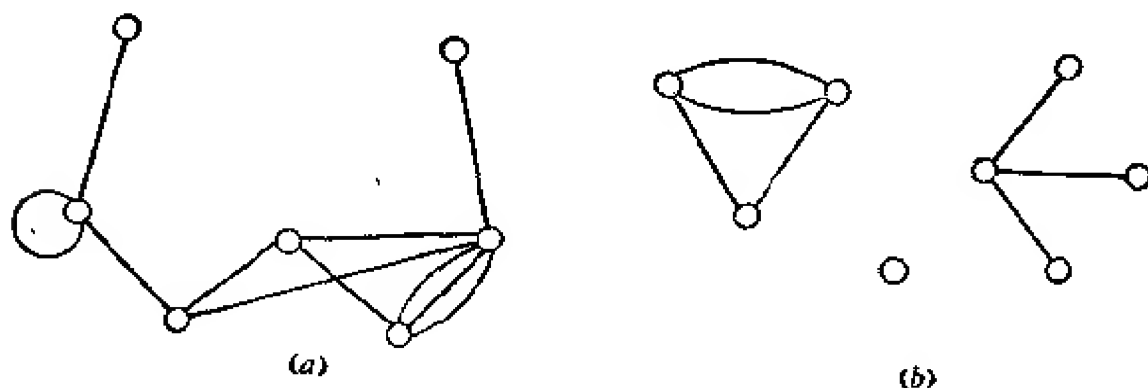


图 7-2.2

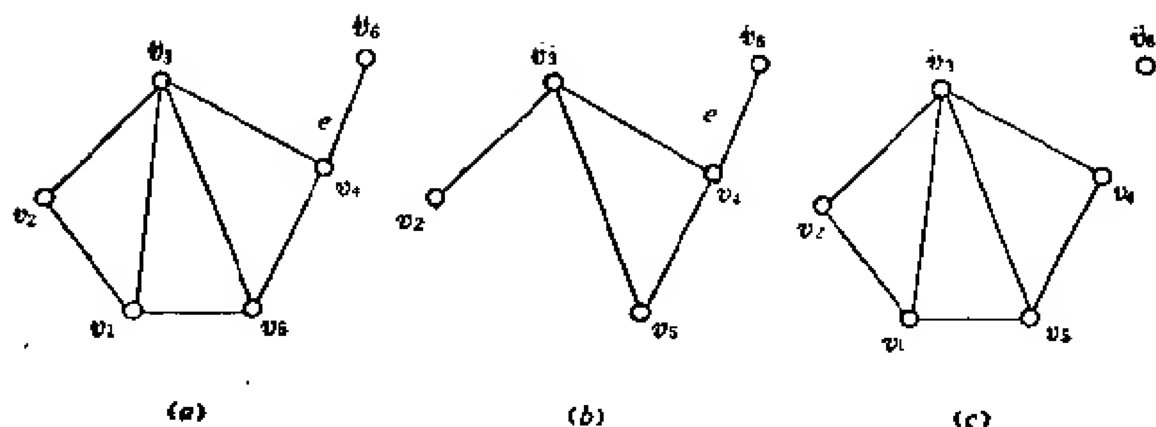


图 7-2.3

图中删除某边，仅需把该边删去。例如，在图 7-2.3(a) 中删除边 e，即由图 (a) 变为图 (c)。

定义 7-2.4 设无向图 $G=\langle V, E\rangle$ 为连通图，若有点集 $V_1\subset V$，使图 G 删除了 V_1 的所有结点后，所得的子图是不连通图，而删除了 V_1 的任何真子集后，所得到的子图仍是连通图，则称 V_1 是 G 的一个点割集。若某一个结点构成一个点割集，则称该结点为割点。

如图 7-2.4(a) 中移去割点 s 后，成为有两个连通分支的非连通图 (b)。

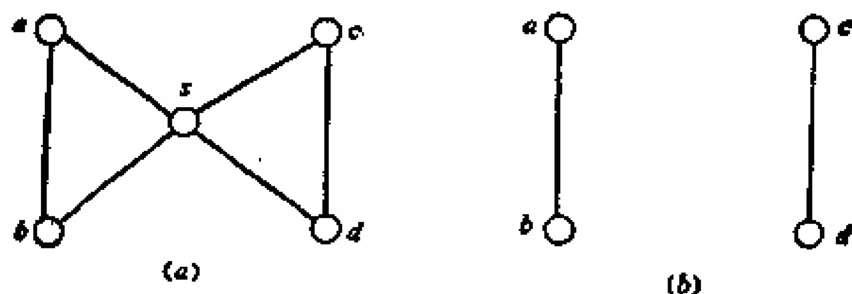


图 7-2.4

若 G 不是完全图，我们定义 $k(G)=\min\{|V_1|\,\big|\,V_1$ 是 G 的点割集$\}$ 为 G 的点连通度（或连通度）。连通度 $k(G)$ 是为了产生一个不连通图需要删去的点的最少数目。于是一个不连通图的连通度等于 0，存在割点的连通图其连通度为 1。完全图 K_p 中，删去任何 m 个 $(m<p-1)$ 点后仍是连通图，但是删去了 $p-1$ 个点后产生

了一个平凡图，故定义 $k(K_p)=p-1$。

定义 7-2.5 设无向图 $G=\langle V, E\rangle$ 为连通图，若有边集 $E_1\subset E$，使图 G 中删除了 E_1 中的所有边后得到的子图是不连通图，而删除了 E_1 的任一真子集后得到的子图是连通图，则称 E_1 是 G 的一个边割集。若某一个边构成一个边割集，则称该边为割边（或桥）。

G 的割边也就是 G 的一条边 e 使 $W(G-e)>W(G)$。与点连通度相似，我们定义非平凡图 G 的边连通度为：$\lambda(G)=\min\{|E_1| \mid E_1$ 是 G 的边割集$\}$，边连通度 $\lambda(G)$ 是为了产生一个不连通图需要删去的边的最少数目。对平凡图 G 可定义 $\lambda(G)=0$，此外一个不连通图也有 $\lambda(G)=0$。

定理 7-2.2 对于任何一个图 G，有

$$k(G)\leqslant\lambda(G)\leqslant\delta(G)$$

证明 若 G 不连通，则 $k(G)=\lambda(G)=0$，故上式成立。

若 G 连通，

1) 证明 $\lambda(G)\leqslant\delta(G)$

如果 G 是平凡图，则 $\lambda(G)=0\leqslant\delta(G)$，若 G 是非平凡图，则因每一结点的所有关联边构成一个边割集，故 $\lambda(G)\leqslant\delta(G)$。

2) 再证 $k(G)\leqslant\lambda(G)$

(a) 设 $\lambda(G)=1$，即 G 有一割边，显然这时 $k(G)=1$，上式成立。

(b) 设 $\lambda(G)\geqslant 2$，则必可删去某 $\lambda(G)$ 条边，使 G 不连通，而删去其中 $\lambda(G)-1$ 条边，它仍是连通的，且有一条桥 $e=(u, v)$。对 $\lambda(G)-1$ 条边中的每一条边都选取一个不同于 u, v 的端点，把这些端点删去则必至少删去 $\lambda(G)-1$ 条边。若这样产生的图是不连通的，则 $k(G)\leqslant\lambda(G)-1<\lambda(G)$，若这样产生的图是连通的，则 e 仍是桥，此时再删去 u 或 v，就必产生一个不连通图，故 $k(G)\leqslant\lambda(G)$。

由 1) 和 2) 得 $k(G)\leqslant\lambda(G)\leqslant\delta(G)$ □

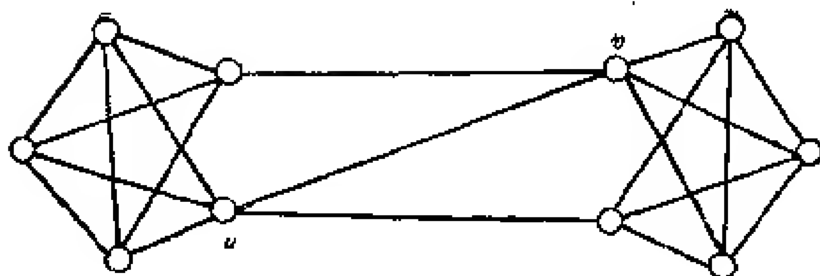


图 7-2.5

这个定理的证明可用图 7-2.5 来予以说明。这里：$k(G)=2$, $\lambda(G)=3$, $\delta(G)=4$。

定理 7-2.3 一个连通无向图 G 中的结点 v 是割点的充分必要条件是存在两个结点 u 和 w，使得结点 u 和 w 的每一条路都通过 v。

证明　若结点 v 是连通图 $G=\langle V, E\rangle$ 的一个割点，设删去 v 得到子图 G'，则 G' 至少包含两个连通分支。设其为 $G_1=\langle V_1, E_1\rangle$, $G_2=\langle V_2, E_2\rangle$，任取 $u\in V_1$, $w\in V_2$，因为 G 是连通的，故在 G 中必有一条连结 u 和 w 的路 C，但 u 和 w 在 G' 中属于两个不同的连通分支，故 u 和 w 必不连通，因此 C 必须通过 v，故 u 和 w 之间的任意一条路都通过 v。

反之，若连接图 G 中某两个结点的每一条路都通过 v，删去 v 得到子图 G'，在 G' 中这两个结点必然不连通，故 v 是图 G 的割点。 □

无向图的连通性，不能直接推广到有向图。在有向图 $G=\langle V, E\rangle$ 中，从结点 u 到 v 有一条路，称从 u 可达 v。可达性是有向图结点集上的二元关系，它是自反和传递的，但一般来说它不是对称的，因为如果从 u 到 v 有一条路，不一定必有 v 到 u 的一条路，故可达性不是等价关系。

如果 u 可达 v，它们之间可能不止一条路，在所有这些路中，最短路的长度称为结点 u 和 v 之间的距离(或短程线)，记作 $d\langle u, v\rangle$，它满足下列性质：

$$d\langle u, v\rangle \geqslant 0$$

$$d\langle u, u\rangle = 0$$

$$d\langle u, v\rangle + d\langle v, w\rangle \geqslant d\langle u, w\rangle$$

如果从 u 到 v 是不可达的，则通常写成 $d\langle u, v\rangle=\infty$。注意当 u 可达 v，且 v 也可达 u 时，$d\langle u, v\rangle$ 不一定等于 $d\langle v, u\rangle$。有关距离的概念对无向图亦适用，今后我们把 $D=\max\limits_{u,v\in V} d\langle u, v\rangle$ 称作图的直径。

定义 7-2.6 在简单有向图 G 中，任何一对结点间，至少有一个结点到另一个结点是可达的，则称这个图是单侧连通的。如果对于图 G 中的任何一对结点两者之间是相互可达的，则称这个图是强连通的。如果在图 G 中略去边的方向，将它看成无向图后，图是连通的，则称该图为弱连通的。

例如图 7-2.6 中分别给出了强连通图 (a)，单侧连通图 (b)，弱连通图 (c)。

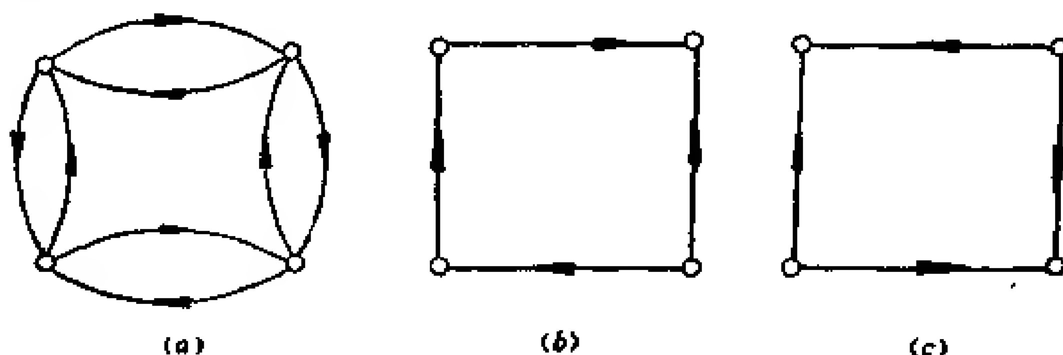


图 7-2.6

从上述定义可以看出，若图 G 是强连通的，则必是单侧连通的；若图 G 是单侧连通的，则必是弱连通的。这两个命题，其逆不真。

定理 7-2.4 一个有向图是强连通的，当且仅当 G 中有一个回路，它至少包含每个结点一次。

证明 充分性

如果 G 中有一个回路，它至少包含每个结点一次，则 G 中任两个结点都是相互可达的，故 G 是强连通图。

必要性

如果有向图 G 是强连通的，则任两个结点都是相互可达。故必可作一回路经过图中所有各点。若不然则必有一回路不包含某

一结点 v，因此，v 与回路上的各结点就不是相互可达，与强连通条件矛盾。 □

定义 7-2.7 在简单有向图中，具有强连通性质的最大子图，称为强分图；具有单侧连通性质的最大子图，称为单侧分图；具有弱连通性质的最大子图，称为弱分图。

例如在图 7-2.7(*a*)中，由 $\{v_1, v_2, v_3, v_4\}$ 或 $\{v_5\}$ 导出的子图都是强分图，由 $\{v_1, v_2, v_3, v_4, v_5\}$ 导出的子图是单侧分图也是弱分图。

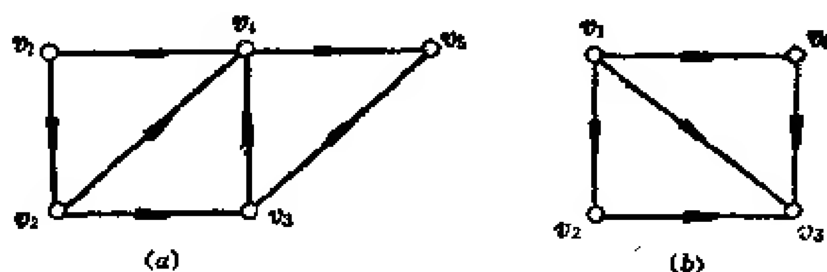


图 7-2.7

又如在图 7-2.7(*b*)中，强分图可由 $\{v_1\}$，$\{v_2\}$，$\{v_3\}$，$\{v_4\}$ 导出，单侧分图可由 $\{v_1, v_2, v_3\}$，$\{v_1, v_3, v_4\}$ 导出，弱分图可由 $\{v_1, v_2, v_3, v_4\}$ 导出。

定理 7-2.5 在有向图 $G=\langle V, E\rangle$ 中，它的每一个结点位于且只位于一个强分图中。

证明 1) 假设 $v\in V$，令 S 是 G 中所有与 v 相互可达的结点的集合，当然 v 也在 S 之中，而 S 是 G 的一个强分图，因此 G 的每一结点必位于一个强分图中。

2) 假设 v 位于两个不同的强分图 S_1 与 S_2 之中，因为 S_1 中每个结点与 v 相互可达，而 v 与 S_2 中每个结点也相互可达，故 S_1 中任何一结点与 S_2 中任何一个结点通过 v 都相互可达，这与题设 S_1 为强分图矛盾。故 G 的每一结点只能位于一个强分图之中。

□

7-2 习题

(1) 在无向图 G 中，从结点 u 到结点 v 有一条长度为偶数的通路，从结点 u 到结点 v 又有一条长度为奇数的通路，则在 G 中必有一条长度为奇数的

回路。

(2) 若无向图 G 中恰有两个奇数度的结点，则这两结点间必有一条路。

(3) 若图 G 是不连通的，则 G 的补图 $\overline{G}$ 是连通的。

(4) 当且仅当 G 的一条边 e 不包含在 G 的回路中时，e 才是 G 的割边。

(5) 分析图 7-2.8，求：

a) 从 A 到 F 的所有通路。

b) 从 A 到 F 的所有迹。

c) A 和 F 之间的距离。

d) $k(G)$，$\lambda(G)$ 和 $\delta(G)$。

图 7-2.8

(6) 令 G 是一个至少有三个结点的连通图，下列命题是等价的。

a) G 没有桥。

b) G 的每二个结点在一条公共的闭迹上。

c) G 的每一个结点和一条边在一条公共的闭迹上。

d) G 的每二条边在一条公共的闭迹上。

e) 对 G 的每一对结点和每一条边，有一条联结这两个结点而且含有这条边的迹。

f) 对 G 的每一对结点和每一条边，有一条联结这两个结点而不含有这条边的通路。

g) 对每三个结点，有一条联结任何两个结点而且含第三个结点的迹。

(7) 在图 7-2.9 中给出了一个有向图，试求 $d\langle v_1, v_4\rangle$，$d\langle v_2, v_5\rangle$ 及 $d\langle v_3, v_6\rangle$。此有向图对应的关系是否可传递的？如果不是可传递的，试求此图的传递闭包。

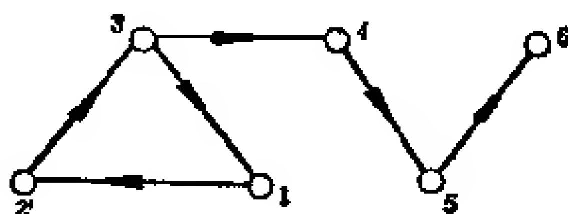


图 7-2.9

(8) 试求图 7-2.9 中的有向图的强分图，单侧分图和弱分图。

(9) 一个有向图 D 是单侧迹通的，当且仅当它有一条经过每一结点的路。

(10) 试证明图的每一个结点和每一条边，都只包含于一个弱分图中。

7-3 图的矩阵表示

在第三章中，对于给定集合 A 上的关系 R，可用一个有向图

表示，这种图形表示了集合 A 上元素之间的关系，关系图亦表示了集合中元素间的邻接关系。对于关系图，可用一个矩阵表示，一个矩阵也必对应于一个标定结点序号的关系图。

定义 7-3.1 设 $G=\langle V, E\rangle$ 是一个简单图，它有 n 个结点 $V=\{v_1, v_2, \cdots, v_n\}$，则 n 阶方阵 $A(G)=(a_{ij})$ 称为 G 的邻接矩阵。

其中
$$a_{ij}=\begin{cases}1 & v_i \ \text{adj} v_j \\ 0 & v_i \ \text{nadj} \ v_j \text{或} i=j\end{cases}$$

adj 表示邻接，nadj 表示不邻接。

例如图 7-3.1，它的邻接矩阵为：

$$A(G)=\begin{bmatrix}0&1&1&1&1\\1&0&1&0&0\\1&1&0&1&0\\1&0&1&0&1\\1&0&0&1&0\end{bmatrix}$$

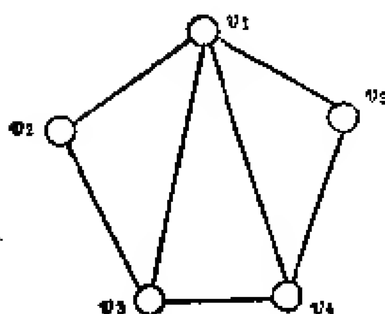


图 7-3.1

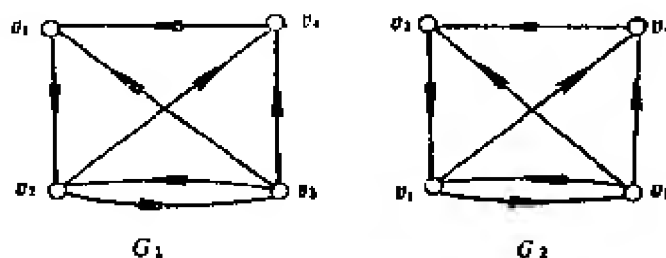


图 7-3.2

当给定的简单图是无向图时，邻接矩阵为对称的，当给定图是有向图时，邻接矩阵并不一定对称。图 G 的邻接矩阵显然与 n 个结点的标定次序$\{v_1, v_2, \cdots, v_n\}$有关。例如图 7-3.2 中，若将结点 v_1 和 v_2 的次序调换一下，那么新的邻接矩阵将是原邻接矩阵第一、二行对调，第一、二列对调而得到。

$$A(G_1)=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{bmatrix} \qquad A(G_2)=\begin{bmatrix}0&0&1&1\\1&0&0&0\\1&1&0&1\\0&1&0&0\end{bmatrix}$$

一般地说，我们把一个 n 阶方阵 A 的某些列作一置换，再把相应的行作同样置换，得到一个新的 n 阶方阵 A'，我们称 A' 与 A 置换等价。显然置换等价是 n 阶布尔矩阵集合上的一个等价关系。有向图的结点，按不同次序所写出的邻接矩阵是彼此置换等价的，今后我们略去这种元素次序的任意性，可取图的任意一个邻接矩阵作为该图的矩阵表示。

从邻接矩阵 A 中，我们看到，第 i 行元素是由结点 v_i 出发的边所决定，第 i 行中值为 1 的元素数目等于 v_i 的出度。同理，在第 j 列中值为 1 的元素数目是 v_j 的入度。

如果给定的一个图是零图，则其对应的矩阵中，所有元素都为零，即它是一个零矩阵，反之亦然。

从图 G 的邻接矩阵中，我们还可以得到图的很多重要性质：

设有向图 G 的结点集合 $V=\{v_1, v_2, \cdots, v_n\}$，它的邻接矩阵为：$A(G)=(a_{ij})_{n\times n}$，现在我们想计算从结点 v_i 到结点 v_j 的长度为 2 的路的数目。注意到每条从 v_i 到 v_j 的长度为 2 的路，中间必须经过一个结点 v_k，即 $v_i\to v_k\to v_j$ $(1\leqslant k\leqslant n)$，如果图 G 中有路 $v_iv_kv_j$ 存在，那么 $a_{ik}=a_{kj}=1$ 即 $a_{ik}\cdot a_{kj}=1$，反之如果图 G 中不存在路 $v_iv_kv_j$，那么 $a_{ik}=0$ 或 $a_{kj}=0$，即 $a_{ik}\cdot a_{kj}=0$。于是从结点 v_i 到结点 v_j 的长度为 2 的路的数目等于：

$$a_{i1}\cdot a_{1j}+a_{i2}\cdot a_{2j}+\cdots+a_{in}\cdot a_{nj}=\sum_{k=1}^{n} a_{ik}\cdot a_{kj}$$

按照矩阵的乘法规则，这恰好等于矩阵 $(A(G))^2$ 中第 i 行，第 j 列的元素。

$$(a_{ij}^{(2)})_{n\times n}=(A(G))^2=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}\cdot\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$a_{ij}^{(2)}$ 表示从 v_i 到 v_j 的长度为 2 的路的数目。

$a_{ii}^{(2)}$ 表示从 v_i 到 v_i 的长度为 2 的回路数目。

从 v_i 到 v_j 的长度为 3 的路，可以看作是由 v_i 到 v_k 的一条长度为 1 的路，再联结 v_k 到 v_j 的一条长度为 2 的路，故 v_i 到 v_j 的长

度为 3 的路的数目：

$$a_{ij}^{(3)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj}^{(2)}$$

即 $\qquad (a_{ij}^{(3)})_{n\times n}=(A(G))^3=(A(G))\cdot(A(G))^2$。

一般地有：

$$(a_{ij}^{(l)})_{n\times n}=(A(G))^l=\overbrace{\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix}\cdots\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix}}^{l}$$

上述这个结论对无向图也成立。

定理 7-3.1 设 (AG) 是图 G 的邻接矩阵，则 $(A(G))^l$ 中的 i 行，j 列元素 $a_{ij}^{(l)}$ 等于 G 中联结 v_i 与 v_j 的长度为 l 的路的数目。

证明 对 l 用数学归纳法

当 $l=2$ 时，由上可知显然成立。

设命题对 l 成立，由

$$(A(G))^{l+1}=A(G)\cdot(A(G))^l$$

故

$$a_{ij}^{(l+1)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj}^{(l)}$$

根据邻接矩阵定义 a_{ik} 表示联结 v_i 与 v_k 的长度为 1 的路的数目，$a_{kj}^{(l)}$ 是联结 v_k 与 v_j 的长度为 l 的路的数目，故上式右边的每一项表示由 v_i 经过一条边到 v_k，再由 v_k 经过一条长度为 l 的路到 v_j 的总长度为 $l+1$ 的路的数目。对所有 k 求和，即得 $a_{ij}^{(l+1)}$ 是所有从 v_i 到 v_j 的长度为 $l+1$ 的路的数目，故命题对 $l+1$ 成立。 □

例 1 给定一图 $G=\langle V, E\rangle$ 如图 7-3.3 所示。

$$A=\begin{bmatrix}0&1&0&0&0\\1&0&1&0&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}\qquad A^2=\begin{bmatrix}1&0&1&0&0\\0&2&0&0&0\\1&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$A^3=\begin{bmatrix}0&2&0&0&0\\2&0&2&0&0\\0&2&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}\qquad A^4=\begin{bmatrix}2&0&2&0&0\\0&4&0&0&0\\2&0&2&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

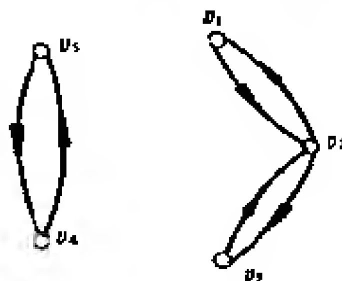


图 7-3.3

从上述矩阵中我们可以得到一些结论，如 v_1 与 v_2 之间有 2 条长度为 3 的路，结点 v_1 与 v_3 之间有一条长度为 2 的路，在结点 v_2 有四条长度为 4 的回路，但没有长度为 3 的回路。

在许多实际问题中，常常要判断有向图的一个结点 v_i 到另一结点 v_j 是否存在路的问题。如果利用图 G 的邻接矩阵 A，则可计算 A, A^2, …, A^n, …，当发现其中某个 A^l 的 $a_{ij}^{(l)}\geq 1$，就表明结点 v_i 到 v_j 可达。但这种计算比较繁琐且 A^l 不知计算到何时为止，根据定理 7-2.1 的推论可知，如果有向图 G 有 n 个结点

$$V=\{v_1,\ v_2,\ \cdots,\ v_n\},$$

v_i 到 v_j 有一条路，则必然有一条长度不超过 n 的通路，因此只要考察 $a_{ij}^{(l)}$ 就可以了，其中 $1\leq l\leq n$。对于有向图 G 中任意两个结点之间的可达性，亦可用矩阵表达。

定义 7-3.2 令 $G=\langle V,\ E\rangle$ 是一个简单有向图，$|V|=n$，假定 G 的结点已编序，即 $V=\{v_1,\ v_2,\ \cdots,\ v_n\}$，定义一个 $n\times n$ 矩阵 $P=(p_{ij})$。

其中 $$p_{ij}=\begin{cases}1 & \text{从 } v_i \text{ 到 } v_j \text{ 至少存在一条路}\\ 0 & \text{从 } v_i \text{ 到 } v_j \text{ 不存在路}\end{cases}$$

称矩阵 P 是图 G 的可达性矩阵。

可达性矩阵表明了图中任意两个结点间是否至少存在一条路

以及在任何结点上是否存在回路。

一般地讲，可由图 G 的邻接矩阵 A 得到可达性矩阵 P，即令 $B_n=A+A^2+\cdots+A^n$，再从 B_n 中将不为零的元素均改换为 1，而为零的元素不变，这个改换的矩阵即为可达性矩阵 P。

例题 1 设图 G 的邻接矩阵为 $A=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{bmatrix}$，求 G 的可达性矩阵。

解 $$A^2=\begin{bmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{bmatrix}\qquad A^3=\begin{bmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{bmatrix}$$

$$A^4=\begin{bmatrix}1&2&1&1\\2&2&2&3\\3&3&2&3\\2&1&0&1\end{bmatrix}$$

故 $$B_4=A+A^2+A^3+A^4=\begin{bmatrix}3&4&2&3\\5&5&4&6\\7&7&4&7\\3&2&1&2\end{bmatrix}$$

$$P=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$$

由此可知图 G 中任两结点间均是可达的，并且任一结点均有回路，因而此图是个连通图。

上述计算可达性矩阵的方法还是比较复杂，因为可达性矩阵是一个元素为 1 或 0 的布尔矩阵，由于在每个 A^i 矩阵中，对于两个结点间具有路的数目不感兴趣，它所关心的是该两结点间是否有路存在，因此我们可将矩阵 A, A^2, $\cdots$, A^n, 分别改为布尔矩阵 $A^{(1)}$, $A^{(2)}$, $\cdots$, $A^{(n)}$，故 $P=A^{(1)}\vee A^{(2)}\vee\cdots\vee A^{(n)}$，其中 $A^{(i)}$ 表示在布尔运算意义下 A 的 i 次方。

例题 2 设图 G 如图 7-3.4 所示，求可达性矩阵 P。

解

$$A=\begin{bmatrix}0&1&0&0&0\\0&0&0&1&0\\1&0&0&0&0\\0&0&0&0&1\\0&1&0&0&0\end{bmatrix}$$

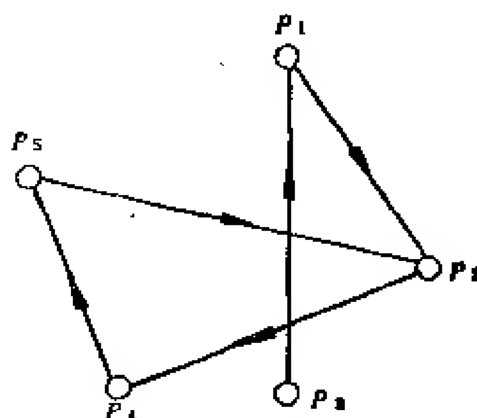


图 7-3.4

$$A^{(2)}=\begin{bmatrix}0&1&0&0&0\\0&0&0&1&0\\1&0&0&0&0\\0&0&0&0&1\\0&1&0&0&0\end{bmatrix}\begin{bmatrix}0&1&0&0&0\\0&0&0&1&0\\1&0&0&0&0\\0&0&0&0&1\\0&1&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&1&0&0&0\\0&0&0&0&1\end{bmatrix}$$

$$A^{(3)}=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&1&0&0&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}0&1&0&0&0\\0&0&0&1&0\\1&0&0&0&0\\0&0&0&0&1\\0&1&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&0&1\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

同理可得：

$$A^{(4)}=\begin{bmatrix}0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&0&0&0&1\\0&1&0&0&0\end{bmatrix}\qquad A^{(5)}=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&1&0&0&0\\0&0&0&1&0\end{bmatrix}$$

$$P=A\vee A^{(2)}\vee A^{(3)}\vee A^{(4)}\vee A^{(5)}=\begin{bmatrix}0&1&0&1&1\\0&1&0&1&1\\0&1&0&1&1\\0&1&0&1&1\\0&1&0&1&1\end{bmatrix}$$

从本例的运算可以看到，如果把邻接矩阵看作是结点集 V 上关系 R 的关系矩阵，则可达性矩阵 P 即为 M_{R^+}，因此可达性矩阵 P 亦可用 Warshall 算法计算。

上述可达性矩阵等概念，可以很容易地推广到无向图中，只要

将无向图中每条无向边看成是具有相反方向的两条边，这样，一个无向图就可看成一个有向图。无向图的邻接矩阵是一个对称矩阵，其可达性矩阵称为连通矩阵，也是对称的。

对于一个无向图 G，除了可用邻接矩阵表示外，还对应着一个称为图 G 的完全关联矩阵，假定图 G 无自回路，如因某种运算得到了自回路，则将它删去。

定义 7-3.3 给定无向图 G，令 $v_1, v_2, \cdots, v_p$ 和 $e_1, e_2, \cdots, e_q$ 分别记为 G 的结点和边，则矩阵 $M(G)=(m_{ij})$，其中

$$m_{ij}=\begin{cases}1 & 若\ v_i\ 关联\ e_j\\ 0 & 若\ v_i\ 不关联\ e_j\end{cases}$$

称 G 为完全关联矩阵。

例如对于图 7-3.5，可写出其关联矩阵：

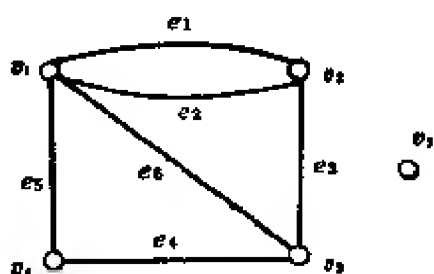


图 7-3.5

	e_1	e_2	e_3	e_4	e_5	e_6
v_1	1	1	0	0	1	1
v_2	1	1	1	0	0	0
v_3	0	0	1	1	0	1
v_4	0	0	0	1	1	0
v_5	0	0	0	0	0	0

从关联矩阵中可以看出图形的一些性质：

1) 图中每一边关联两个结点，故 $M(G)$ 的每一列中只有两个 1。

2) 每一行中元素的和数是对应结点的度数。

3) 一行中元素全为 0，其对应的结点为孤立结点。

4) 两个平行边其对应的两列相同。

5) 同一个图当结点或边的编序不同时，其对应的 $M(G)$ 仅有行序，列序的差别。

当一个图是有向图时，亦可用结点和边的关联矩阵表示。

定义 7-3.4 给定简单有向图

$G=\langle V, E\rangle$，$V=\{v_1, v_2, \cdots, v_p\}$，$E=\{e_1, e_2, \cdots, e_q\}$，

$p\times q$ 阶矩阵 $M(G)=(m_{ij})$，其中

$$m_{ij}=\begin{cases}1 & \text{若在 } G \text{ 中 } v_i \text{ 是 } e_j \text{ 的起点} \\ -1 & \text{若在 } G \text{ 中 } v_i \text{ 是 } e_j \text{ 的终点} \\ 0 & \text{若 } v_i \text{ 与 } e_j \text{ 不关联}\end{cases}$$

称 $M(G)$ 为 G 的完全关联矩阵。

例如由图 7-3.6 可写出其关联矩阵：

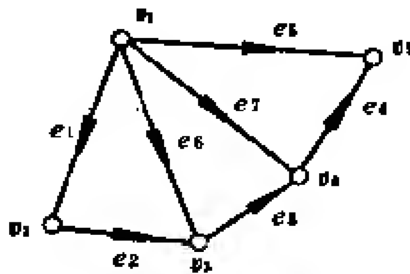


图 7-3.6

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
v_1	1	0	0	0	1	1	1
v_2	−1	1	0	0	0	0	0
v_3	0	−1	1	0	0	−1	0
v_4	0	0	−1	1	0	0	−1
v_5	0	0	0	−1	−1	0	0

有向图的完全关联矩阵也有类似于无向图的一些性质，读者可试予归纳。

对图 G 的完全关联矩阵中两个行相加定义如下：若记 v_i 对应的行为 $\vec{v}_i$，将第 i 行与第 j 行相加，规定为：对有向图是指对应分量的普通加法运算，对无向图是指对应分量的模 2 加法运算，把这种运算记作 $\vec{v}_i\oplus\vec{v}_j=\vec{v}_{ij}$。施行这种运算，实际上就是相应于把 G 的结点 v_i 与 v_j 合并。

设图 G 的结点 v_i 与 v_j 合并得到图 G'，那么 $M(G')$ 是将 $M(G)$ 中 $\vec{v}_i$ 与 $\vec{v}_j$ 相加而得到。因为若有关项中第 r 个对应分量有 $a_{ir}\oplus a_{jr}=\pm1$，则说明 v_i 和 v_j 两者之中只有一个结点是边 e_r 的端点，且将两个结点合并后的结点 $v_{i,j}$ 仍是 e_r 的端点。

若 $a_{ir}\oplus a_{jr}=0$，则有两种情况：

a) v_i, v_j 都不是 e_r 的端点，那么 $v_{i,j}$ 也不是 e_r 的端点。

b) v_i, v_j 都是 e_r 的端点，那么合并后在 G' 中 e_r 成为 $v_{i,j}$ 的自回路，按规定应删去。

此外，在 $M(G')$ 中若有某些列，其元素全为零，说明由 G 中的一些结点合并后，消失了一些对应边。

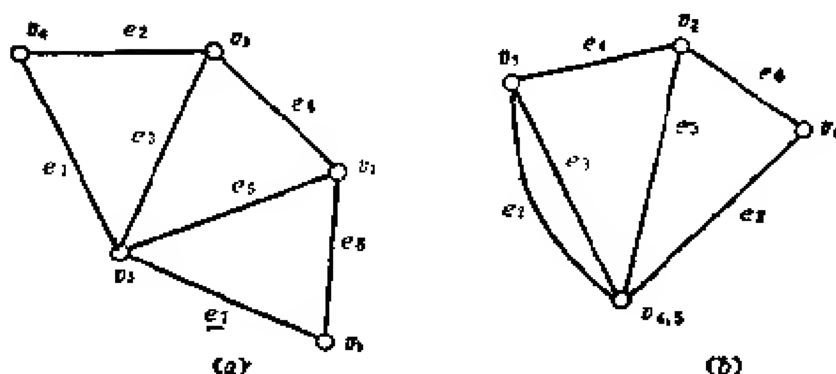


图 7-3.7

例1 图 7-3.7(a)中使 v_4 与 v_5 合并得到图 7-3.7(b)

其关联矩阵 $M(G')$是由 $M(G)$中将第 4 行加到第 5 行而得到。

$M(G)$:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
v_1	0	0	0	0	0	1	1
v_2	0	0	0	1	1	1	0
v_3	0	1	1	1	0	0	0
v_4	1	1	0	0	0	0	0
v_5	1	0	1	0	1	0	1

$M(G')$:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
v_1	0	0	0	0	0	1	1
v_2	0	0	0	1	1	1	0
v_3	0	1	1	1	0	0	0
$v_{4,5}$	0	1	1	0	1	0	1

例2 图 7-3.8(a) 合并结点 v_2 和 v_3, 删去自回路得图 7-3.8(b)。

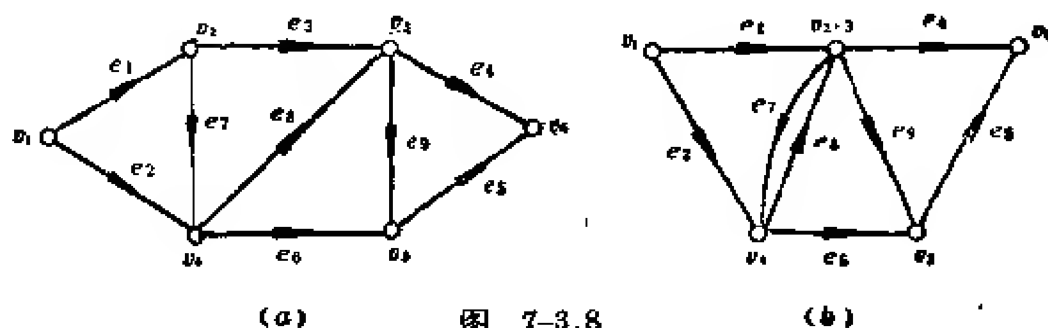


图 7-3.8

其关联矩阵 $M(G')$ 是由 $M(G)$ 中将第 2 行加到第 3 行而得到。

$M(G)$:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9
v_1	1	1	0	0	0	0	0	0	0
v_2	−1	0	1	0	0	0	1	0	0
v_3	0	0	−1	1	0	0	0	−1	1
v_4	0	−1	0	0	0	1	−1	1	0
v_5	0	0	0	0	1	−1	0	0	−1
v_6	0	0	0	−1	−1	0	0	0	0

$M(G')$:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9
v_1	1	1	0	0	0	0	0	0	0
$v_{2,3}$	−1	0	0	1	0	0	1	−1	1
v_4	0	−1	0	0	0	1	−1	1	0
v_5	0	0	0	0	1	−1	0	0	−1
v_6	0	0	0	−1	−1	0	0	0	0

下面应用这种运算，可求关联矩阵的秩。

定理 7-3.2 如果一个连通图 G 有 r 个结点，则其完全关联矩阵 $M(G)$ 的秩为 $r-1$，即 $\operatorname{rank} M(G)=r-1$。

证明 这里对无向图进行证明。

(1) 由于矩阵 $M(G)$ 的每一列恰有两个 1，若把 $M(G)$ 的其余所有行加到最后一行上(模 2 加法)，得到矩阵 $\overline{M}(G)$，它的最后一行全为零，因为 $\overline{M}(G)$ 的秩与 $M(G)$ 相同，故 $M(G)$ 的秩应小于行数，即 $\operatorname{rank} M(G)\leqslant r-1$。

(2) 设 $M(G)$ 的第一列对应边 e，且 e 的端点为 v_i 和 v_j，调整行序使第 i 行成为第一行，这时 $M(G)$ 的首列仅在第一行和第 j 行为 1，其余各元素均为 0，再把第一行加到第 j 行上去，则得矩阵 $M'(G)$。

$$M'(G)=\left[\begin{array}{c|c}1 & \cdots\ \cdots\ \cdots \\ \hline 0 & \\ \vdots & M'(G_1) \\ 0 & \end{array}\right]$$

其中 $M'(G_1)$ 是 $M'(G)$ 删去第一行和第一列所得的矩阵。

由于 $M'(G_1)$ 是 G_1 的完全关联矩阵，而 G_1 系将 G 的两个结点 v_i 和 v_j 合并而得。由于 G 是连通的，故 G_1 也必为连通，$M'(G_1)$ 也具有连通图的完全关联矩阵的所有性质，故 $M'(G_1)$ 没有全零的行。如果 $M'(G_1)$ 的第一列全为零，则可将 $M'(G_1)$ 中的非零列与第一列对换，而不影响完全关联矩阵的秩数。因此，我们必可通过调整行的次序以及把一行加到另一行上这两种运算，使 $M'(G_1)$ 的第一列的首项元素为 1，得到：

$$M''(G)=\left[\begin{array}{c|c|c}1 & \cdots & \cdots\ \cdots \\ \hline 0 & 1 & \cdots\ \cdots \\ \hline \vdots & 0 & \\ & \vdots & M'(G_2) \\ 0 & 0 & \end{array}\right]$$

继续进行上述两种运算，并不改变矩阵的秩，经过 $r-1$ 次，最后将 $M(G)$ 变换成，

$$M^{(r-1)}(G):=\begin{bmatrix}1 & & & & & & \\ 0 & 1 & & & & & \\ 0 & 0 & 1 & & & & \\ \vdots & \vdots & & \ddots & & & \\ 0 & 0 & \cdots & \cdots 1 & & & \\ 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots\ 0\end{bmatrix}$$

显然 $M^{(r-1)}(G)$ 有一个 $(r-1)$ 阶子阵，其行列式的值不为零，故 $M^{(r-1)}(G)$ 的秩至少为 $r-1$。

由(1)和(2)可知

$$\operatorname{rank} M(G)=r-1 \qquad \square$$

对于有向图的关联矩阵可以仿此证明。

例 3　计算图 7-3.7(*a*)中其对应的完全关联矩阵的秩数，以验证定理 7-3.2。

设有完全关联矩阵 $M(G)$，以 (k) 记第 k 行，以 $\widehat{m}$ 记第 m 列，以 $\widehat{k}\leftrightarrow\widehat{m}$ 表示第 k 列与第 m 列对调，$(k)\leftrightarrow(m)$ 表示第 k 行与第 m 行对调，图 7-3.7(*a*)的完全关联矩阵为

$M(G)$:

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
v_1	0	0	0	0	0	1	1
v_2	0	0	0	1	1	1	0
v_3	0	1	1	1	0	0	0
v_4	1	1	0	0	0	0	0
v_5	1	0	1	0	1	0	1

$$\xrightarrow{(4)\leftrightarrow(1)}\begin{pmatrix}1&1&0&0&0&0&0\\0&0&0&1&1&1&0\\0&1&1&1&0&0&0\\0&0&0&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}\xrightarrow{(1)\oplus(5)}\begin{pmatrix}1&1&0&0&0&0&0\\0&0&0&1&1&1&0\\0&1&1&1&0&0&0\\0&0&0&0&0&1&1\\0&1&1&0&1&0&1\end{pmatrix}$$

$$\xrightarrow{(2)\leftrightarrow(3)}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&1&0&0&0\\0&0&0&1&1&1&0\\0&0&0&0&0&1&1\\0&1&1&0&1&0&1\end{pmatrix}\xrightarrow{(2)\oplus(5)}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&1&0&0&0\\0&0&0&1&1&1&0\\0&0&0&0&0&1&1\\0&0&0&1&1&0&1\end{pmatrix}$$

$$\xrightarrow{\widehat{3}\leftrightarrow\widehat{4}}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&1&0&0&0\\0&0&1&0&1&1&0\\0&0&0&0&0&1&1\\0&0&1&0&1&0&1\end{pmatrix}\xrightarrow{(3)\oplus(5)}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&1&0&0&0\\0&0&1&0&1&1&0\\0&0&0&0&0&1&1\\0&0&0&0&0&1&1\end{pmatrix}$$

$$\xrightarrow{④\leftrightarrow⑥}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&1&0\\0&0&1&1&1&0&0\\0&0&0&1&0&0&1\\0&0&0&1&0&0&1\end{pmatrix}\xrightarrow{(4)\oplus(5)}\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&1&0\\0&0&1&1&1&0&0\\0&0&0&1&0&0&1\\0&0&0&0&0&0&0\end{pmatrix}$$

最后一个矩阵其秩为 4，即 $\text{rank } M(G)=5-1=4$。

推论 设图 G 有 r 个结点，w 个最大连通子图，则图 G 完全关联矩阵的秩为 $r-w$。

7-3 习题

(1) 求出图 7-3.9 中有向图的邻接矩阵 A，找出从 v_1 到 v_4 长度为 2 和 4 的路，用计算 A^2, A^3 和 A^4 来验证这结论。

(2) 对于邻接矩阵 A 的简单有向图 G，它的距离矩阵定义如下：

$d_{ij}=\infty$ 如果 $d\langle v_i, v_j\rangle=\infty$

$d_{ii}=0$ 对所有的 $i=1, 2, \cdots, n$

$d_{ij}=k$ 这里 k 是使 $a_{ij}^{(k)}\neq 0$ 的最小正整数

确定由图 7-3.9 所示的有向图的距离矩阵，并指出 $d_{ij}=1$ 是什么意义？

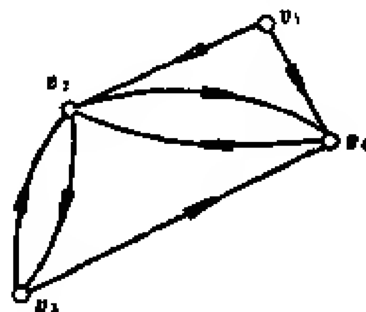


图 7-3.9

(3) 在图 7-3.10 中给出了一个有向图，试求该图的邻接矩阵，并求出可达性矩阵和距离矩阵。

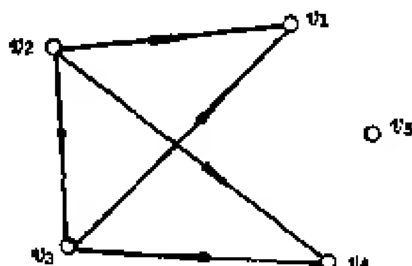


图 7-3.10

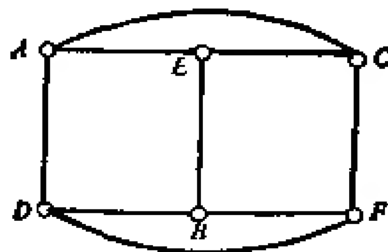


图 7-3.11

(4) 写出如图 7-3.11 所示的图 G 的完全关联矩阵，并验证其秩如定理 7-3.2 所述。

(5) 证明定理 7-3.2 的推论。

7-4 欧拉图与汉密尔顿图

1736 年瑞士数学家列昂哈德·欧拉 (Leonhard Euler) 发表了图论的第一篇论文"哥尼斯堡七桥问题"。这个问题是这样的：哥尼斯堡 (Königsberg) 城市有一条横贯全城的普雷格尔 (Pregel) 河，城的各部分用七座桥联接，每逢假日，城中居民进行环城逛游，这样就产生了一个问题，能不能设计一次"遍游"，使得从某地出发对每座跨河桥只走一次，而在遍历了七桥之后却又能回到原地。在图 7-4.1 中画出了哥尼斯堡城图，城的四个陆地部分分别标以 A、B、C、D。将陆地设想为图的结点，而把桥画成相应的连接边，这样城图可简化成如图 7-4.2 所示，于是遍过哥尼斯堡城中每座桥一次且仅一次的问题，等价于在图 7-4.2 中从某一结点出发找一条通路，通过它的每条边一次且仅一次，并回到原结点。

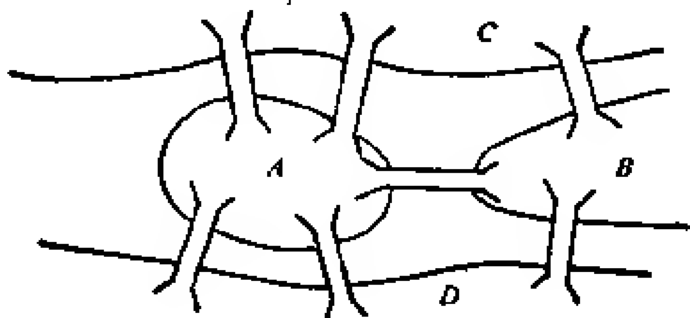


图 7-4.1

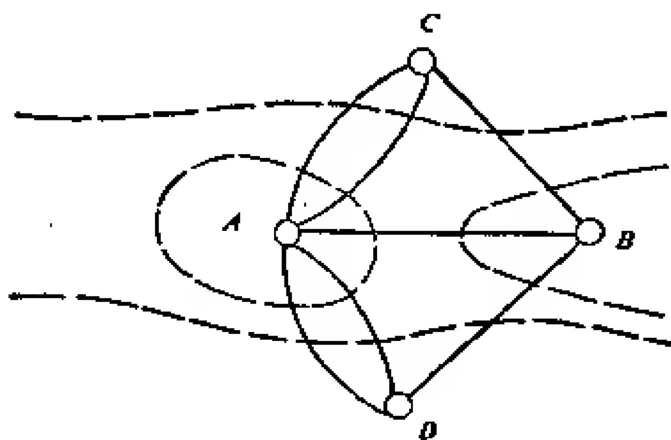


图 7-4.2

欧拉在 1736 年的论文中提出了一条简单的准则，确定了哥尼斯堡七桥问题是不能解的。下面将讨论这个问题的证明。

定义 7-4.1 给定无孤立结点图 G，若存在一条路，经过图中每边一次且仅一次，该条路称为欧拉路；若存在一条回路，经过图中每边一次且仅一次，该回路称为欧拉回路。

具有欧拉回路的图称作欧拉图。

定理 7-4.1 无向图 G 具有一条欧拉路，当且仅当 G 是连通的，且有零个或两个奇数度结点。

证明 必要性

设 G 具有欧拉路，即有点边序列 $v_0e_1v_1e_2v_2\cdots e_iv_ie_{i+1}\cdots e_kv_k$，其中结点可能重复出现，但边不重复，因为欧拉路经过所有图 G 的结点，故图 G 必是连通的。

对任意一个不是端点的结点 v_i，在欧拉路中每当 v_i 出现一次，必关联两条边，故 v_i 虽可重复出现，但 $\deg(v_i)$ 必是偶数。对于端点，若 $v_0=v_k$，则 $d(v_0)$ 为偶数，即 G 中无奇数度结点，若端点 v_0 与 v_k 不同，则 $d(v_0)$ 为奇数，$d(v_k)$ 为奇数，G 中就有两个奇数度结点。

充分性

若图 G 连通，有零个或两个奇欧度结点，我们构造一条欧拉路如下：

(1) 若有两个奇数度结点，则从其中的一个结点开始构造一条迹，即从 v_0 出发经关联边 e_1 "进入" v_1，若 $\deg(v_1)$ 为偶数，则必可由 v_1 再经关联边 e_2 进入 v_2，如此进行下去，每边仅取一次。由于 G 是连通的，故必可到达另一奇数度结点停下，得到一条迹 L_1：$v_0e_1v_1e_2\cdots v_ie_{i+1}\cdots v_k$。若 G 中没有奇数度结点则从任一结点 v_0 出发，用上述方法必可回到结点 v_0，得到上述一条闭迹 L_1。

(2) 若 L_1 通过了 G 的所有边，则 L_1 就是欧拉路。

(3) 若 G 中去掉 L_1 后得到子图 G'，则 G' 中每个结点度数为偶数，因为原来的图是连通的，故 L_1 与 G' 至少有一个结点 v_i 重合，在 G' 中由 v_i 出发重复(1)的方法，得到闭迹 L_2。

(4) 当 L_1 与 L_2 组合在一起，如果恰是 G，则即得欧拉路，否则重复(3)可得到闭迹 L_3，以此类推直到得到一条经过图 G 中所有边的欧拉路。 □

推论 无向图 G 具有一条欧拉回路，当且仅当 G 是连通的，并且所有结点度数全为偶数。

由于有了欧拉路和欧拉回路的判别准则，因此哥尼斯堡七桥问题立即有了确切的否定答案，因为从图7-4.2中可以看到 $\deg(A)=5$，$\deg(B)=\deg(C)=\deg(D)=3$，故欧拉回路必不存在。

与七桥问题类似的还有一笔画的判别问题，要判定一个图 G 是否可一笔画出，有两种情况：一是从图 G 中某一结点出发，经过图 G 的每一边一次仅一次到达另一结点。另一种就是从 G 的某个结点出发，经过 G 的每一边一次仅一次再回到该结点。上述两种情况分别可以由欧拉路和欧拉回路的判定条件予以解决。如图 7-4.3(a)中，因为 $\deg(v_2)=\deg(v_3)=3$，$\deg(v_1)=\deg(v_4)=\deg(v_5)=2$，故必有从 v_2 到 v_3 的一笔画。在图 7-4.3(b) 中所有结点度数均为偶数，所以可以从任一结点出发，一笔画回到原出发点。

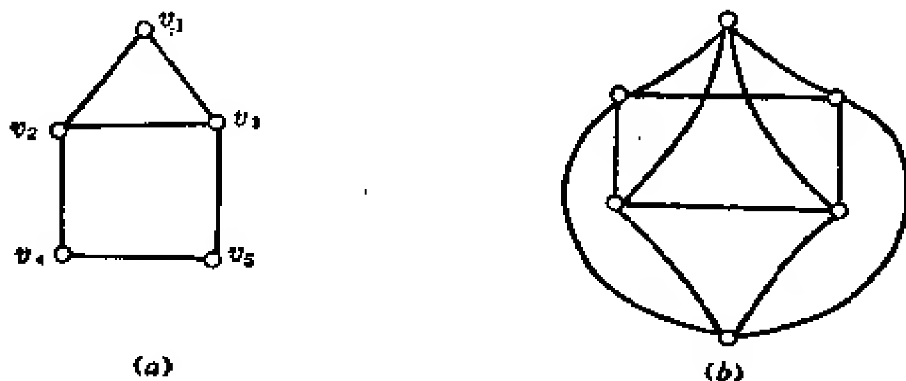


图 7-4.3

欧拉路和欧拉回路的概念，很易推广到有向图中去。

定义 7-4.2 给定有向图 G，通过图中每边一次且仅一次的一条单向路(回路)，称作单向欧拉路(回路)。

定理 7-4.2 有向图 G 具有一条单向欧拉回路，当且仅当是连通的，且每个结点入度等于出度。一个有向图 G 具有单向欧拉路，当且仅当它是连通的，而且除两个结点外，每个结点的入度等于出度，但这两个结点中，一个结点的入度比出度大 1，另一个结点的入度比出度小 1。

这个定理的证明，可以看作是无向图的欧拉路的推广，因为对

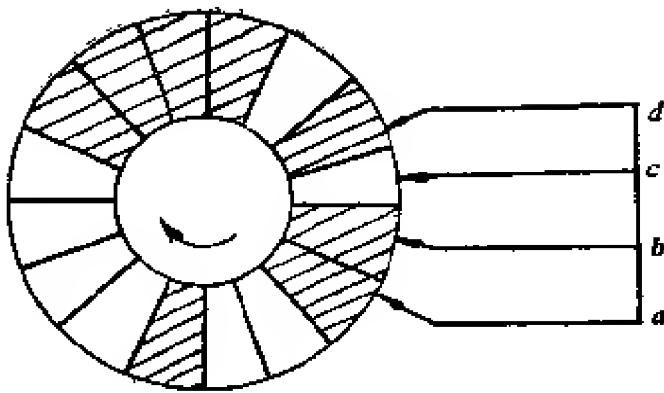


图 7-4.4

于有向图的任意一个结点来说，如果入度与出度相等，则该点的总度数为偶数，若入度与出度之差为1时，其总度数为奇数，因此定理7-4.2的证明与定理7-4.1的证明类似。 □

例1 计算机鼓轮的设计。设有旋转鼓轮其表面被等分成2^4个部分，如图7-4.4所示。

其中每一部分分别用绝缘体或导体组成，绝缘体部分给出信号0，导体部分给出信号1，在图7-4.4中阴影部分表示导体，空白部分表示绝缘体，根据鼓轮的位置，触点将得到信息1101，如果鼓轮沿顺时针方向旋转一个部分，触点将有信息1010。问鼓轮上16个部分怎样安排导体及绝缘体，才能使鼓轮每旋转一个部分，四个触点能得到一组不同的四位二进制数信息。

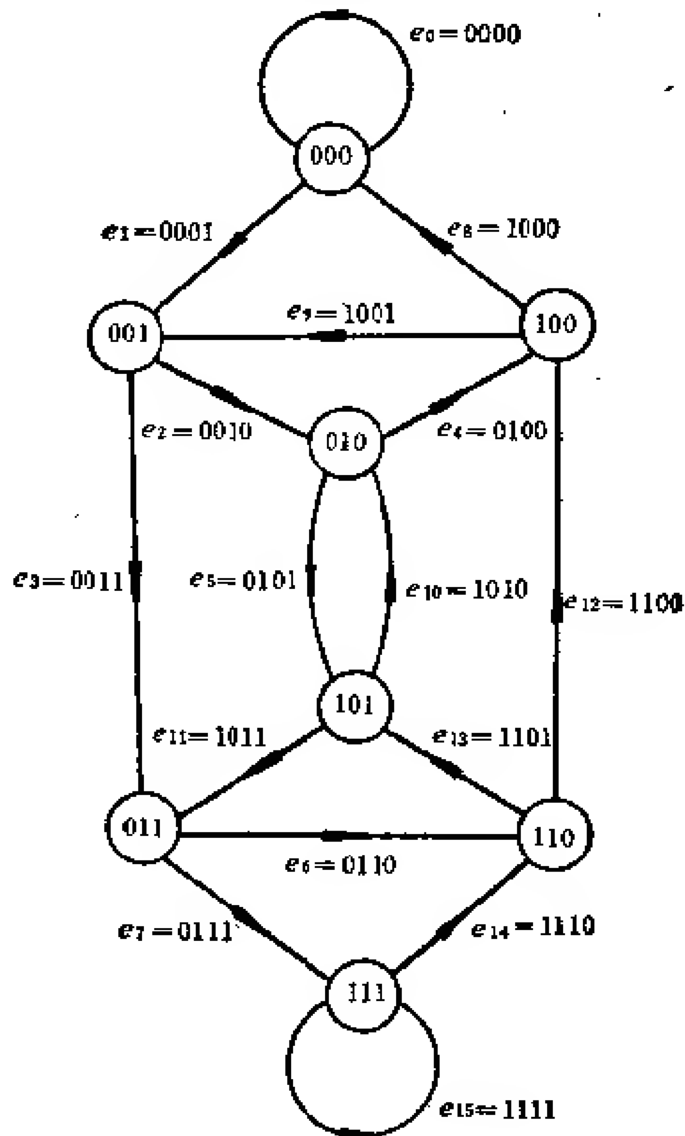


图 7-4.5

设有一个八个结点的有向图（图7-4.5），其结点分别记为三位二进制数{000, 001,

010, 011, 100, 101, 110, 111}，设 $\alpha_i \in \{0, 1\}$，从结点 $\alpha_1\alpha_2\alpha_3$ 可引出两条有向边，其终点分别是 $\alpha_2\alpha_3 0$ 以及 $\alpha_2\alpha_3 1$。该两条边分别记为 $\alpha_1\alpha_2\alpha_3 0$ 和 $\alpha_1\alpha_2\alpha_3 1$。按照上述方法，对于八个结点的有向图共有 16 条边，在这种图的任一条路中，其邻接的边必是 $\alpha_1\alpha_2\alpha_3\alpha_4$ 和 $\alpha_2\alpha_3\alpha_4\alpha_5$ 的形式，即是第一条边标号的后三位数与第二条边标号的头三位数相同。因为图中 16 条边被记成不同的二进制数，可见前述鼓轮转动所得到 16 个不同位置触点上的二进制信息，即对应于图中的一条欧拉回路。在图 7-4.5 中，每个结点的入度等于 2，出度等于 2，故在图中必可找到一条欧拉回路如 $(e_0 e_1 e_2 e_4 e_9 e_3 e_6 e_{13} e_{10} e_5 e_{11} e_7 e_{15} e_{14} e_{12} e_8)$，根据邻接边的标号记法，这 16 个二进制数可写成对应的二进制数序列 0000100110101111。把这个序列排成环状，即与所求的鼓轮相对应，如图 7-4.4 所示。

上面的例子，我们可以把它推广到鼓轮具有 n 个触点的情况。为此我们只要构造 2^{n-1} 个结点的有向图，设每个结点标记为 $n-1$ 位二进制数，从结点 $\alpha_1\alpha_2\cdots\alpha_{n-1}$ 出发，有一条终点为 $\alpha_2\alpha_3\cdots\alpha_{n-1}0$ 的边，该边记为 $\alpha_1\alpha_2\cdots\alpha_{n-1}0$；还有一条边的终点为 $\alpha_2\alpha_3\cdots\alpha_{n-1}1$ 的边，该边记为 $\alpha_1\alpha_2\cdots\alpha_{n-1}1$。这样构造的有向图，其每一结点的出度和入度都是 2，故必是欧拉图。由于邻接边的标记是第一条边的后 $n-1$ 位二进制数与第二条边的前 $n-1$ 位二进制数相同，为此就有一种 2^n 个二进制数的环形排列与所求的鼓轮相对应。

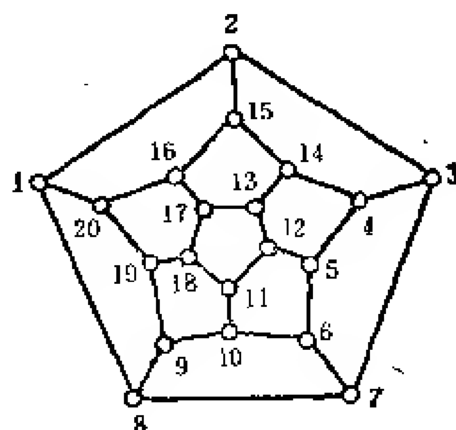


图 7-4.6

与欧拉回路非常类似的问题是汉密尔顿回路的问题。1859 年，威廉·汉密尔顿爵士 (Sir Willian Hamilton)在给他朋友的一封信中，首先谈到关于十二面体的一个数学游戏：能不能在图 7-4.6 中找到一条回路，使它含有这个图的所有结点？他把每个结点看成一个城市，联结两个结点的边看成是交通线，于是他的问题就是能不能找到旅行路线，沿着交通线经过每个

城市恰好一次，再回到原来的出发地？ 他把这个问题称为周游世界问题。

按图 7-4.6 中所给的编号，可以看出这样一条回路是存在的。

对于任何连通图也有类似的问题。

定义 7-4.3 给定图 G，若存在一条路经过图中的每个结点恰好一次，这条路称作汉密尔顿路。若存在一条回路，经过图中的每个结点恰好一次，这条回路称作汉密尔顿回路。

具有汉密尔顿回路的图称作汉密尔顿图。

定理 7-4.3 若图 $G=\langle V, E\rangle$ 具有汉密尔顿回路，则对于结点集 V 的每个非空子集 S 均有 $W(G-S)\leqslant|S|$ 成立。其中 $W(G-S)$ 是 $G-S$ 中连通分支数。

证明 设 C 是 G 的一条汉密尔顿回路，则对于 V 的任何一个非空子集 S 在 C 中删去 S 中任一结点 a_1，则 $C-a_1$ 是连通的非回路，若再删去 S 中另一结点 a_2，则 $W(C-a_1-a_2)\leqslant 2$，由归纳法可得：

$$W(C-S)\leqslant|S|$$

同时 $C-S$ 是 $G-S$ 的一个生成子图，因而

$$W(G-S)\leqslant W(C-S)$$

所以 $$W(G-S)\leqslant|S|$$ □

利用定理 7-4.3 可以证明某些图是非汉密尔顿图。如图 7-4.7 中若取 $S=\{v_1, v_4\}$，则 $G-S$ 中有三个分图，故 G 不是汉密尔顿图。

需要指出，用定理 7-4.3 来证明某一特定图是非汉密尔顿图，

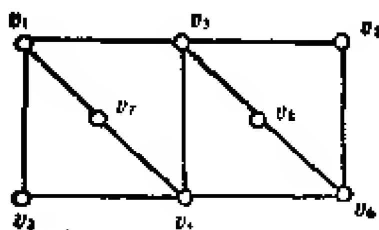


图 7-4.7

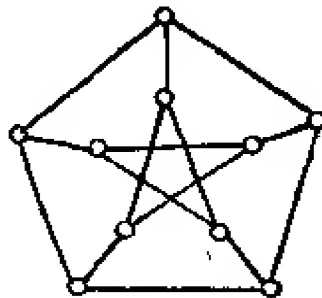


图 7-4.8

这个方法并不是总是有效的。例如，著名的彼得森(Petersen)图，如图 7-4.8 中所示，在图中删去任一个结点或任意两个结点，不能使它不连通；删去 3 个结点，最多只能得到有两个连通分支的子图；删去 4 个结点，只能得到最多三个连通分支的子图；删去 5 个或 5 个以上的结点，余下子图的结点数都不大于 5，故必不能有 5 个以上的连通分支数。所以该图满足 $W(G-S)\leqslant|S|$，但是可以证明它是非汉密尔顿图(此证明留作习题)。

虽然汉密尔顿回路问题与欧拉回路问题在形式上极为相似，但对图 G 是否存在汉密尔顿回路还无充要的判别准则。下面我们给出一个无向图具有汉密尔顿路的充分条件。

定理 7-4.4 设 G 具有 n 个结点的简单图，如果 G 中每一对结点度数之和大于等于 $n-1$，则在 G 中存在一条汉密尔顿路。

证明 我们首先证明 G 是连通图。若 G 有两个或更多个互不连通的分图，设一个分图中有 n_1 个结点，任取一个结点 v_1。设另一个分图中有 n_2 个结点，任取一个结点 v_2，因为 $d(v_1)\leqslant n_1-1$，$d(v_2)\leqslant n_2-1$，故 $d(v_1)+d(v_2)\leqslant n_1+n_2-2<n-1$，这与题设矛盾，故 G 必连通。

其次，我们从一条边出发构成一条路，证明它是汉密尔顿路。

设在 G 中有 $p-1$ 条边的路，$p<n$，它的结点序列为 v_1，v_2，$\cdots$，v_p。如果有 v_1 或 v_p 邻接于不在这条路上的一个结点，我们立刻可扩展这条路，使它包含这一个结点，从而得到 p 条边的路。否则，v_1 和 v_p 都只邻接于这条路上的结点，我们证明在这种情况下，存在一条回路包含结点 v_1，v_2，$\cdots$，v_p。若 v_1 邻接于 v_p，则 v_1，v_2，$\cdots$，v_p，v_1 即为所求的回路。假设与 v_1 邻接的结点集是 $\{\overbrace{v_l, v_m, \cdots, v_j, \cdots, v_t}^{k}\}$，这里 $2\leqslant l, m, \cdots, j, \cdots, t\leqslant p-1$，如果 v_p 是邻接于 v_{l-1}，v_{m-1}，$\cdots$，v_{j-1}，$\cdots$，v_{t-1} 中之一，譬如说 v_{j-1}，如图 7-4.9(*a*)所示，$v_1v_2v_3\cdots v_{j-1}v_pv_{p-1}\cdots v_jv_1$ 是所求的包含结点 v_1，v_2，$\cdots$，v_p 的回路。

如果 v_p 不邻接于 $v_{l-1}, v_{m-1}, \cdots, v_{t-1}$ 中任一个，则 v_p 至多邻接于 $p-k-1$ 个结点，$\deg(v_p)\leqslant p-k-1$，$\deg(v_1)=k$，故 $\deg(v_p)+\deg(v_1)\leqslant p-k-1+k=p-1<n-1$，即 v_1 与 v_p 度数之和至多为 $n-2$，得到矛盾。

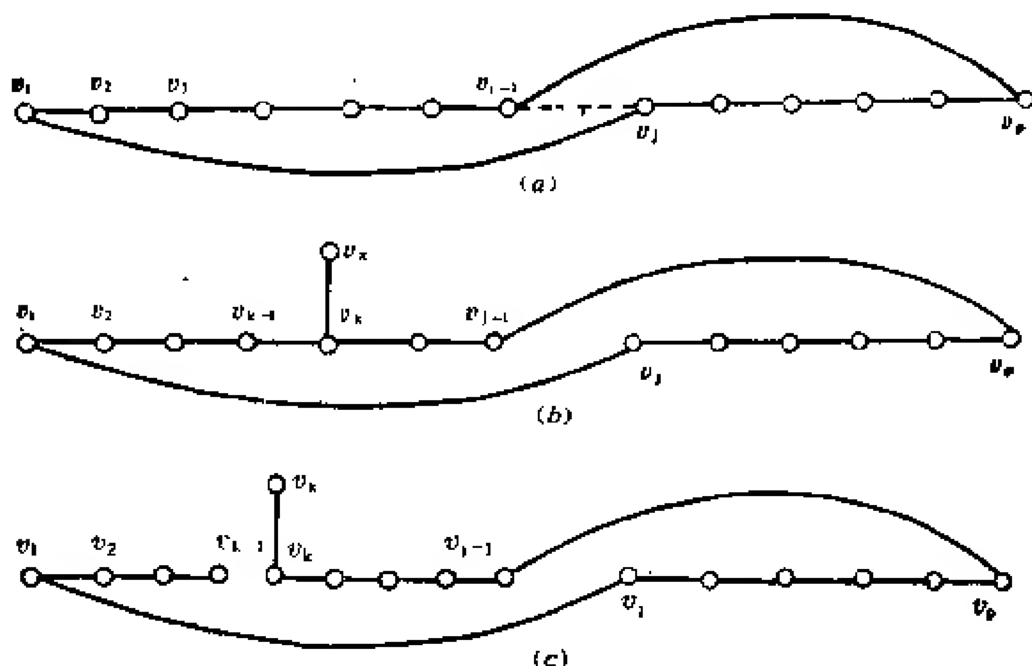


图 7-4.9

至此，我们有包含所有结点 $v_1, v_2, \cdots, v_p$ 的一条回路，因为 G 是连通的，所以在 G 中必有一个不属于该回路的结点 v_x 与 $v_1v_2\cdots v_p$ 中的某一个结点 v_k 邻接，如图 7-4.9(b) 所示，于是就得到一条包含 p 条边的路（$v_x, v_k, v_{k+1}, \cdots, v_{j-1}, v_p, v_{p-1}, \cdots, v_j, v_1, v_2, \cdots, v_{k-1}$）。如图 7-4.9($c$) 所示，重复前述构造法，直到得到 $n-1$ 条边的路。 □

容易看出定理 7-4.4 的条件对于图中汉密尔顿路的存在性只是充分的，但并不是必要条件。设 G 是 n 边形，如图 7-4.10，其中 $n=6$，虽然任何两个结点度数之和是 $4<6-1$，但在 G 中有一条汉密尔顿路。

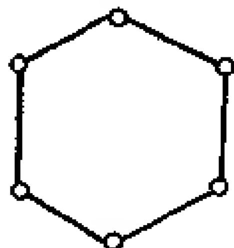


图 7-4.10

例题 1 考虑在七天内安排七门课程的考试，使得同一位教师所任的两门课程考试不排在接连的两天中，试证明如果没有教师担任多于四门课程，则符合上述要求的考试安排总

是可能的。

证明　设G为具有七个结点的图，每个结点对应于一门课程考试，如果这两个结点对应的课程考试是由不同教师担任的，那么这两个结点之间有一条边，因为每个教师所任课程数不超过4，故每个结点的度数至少是3，任两个结点的度数之和至少是6，故G总是包含一条汉密尔顿路，它对应于一个七门考试课目的一个适当的安排。

定理7-4.5　设G是具有n个结点的简单图，如果G中每一对结点度数之和大于等于n，则在G中存在一条汉密尔顿回路。

证明　由定理7-4.4可知必有一条汉密尔顿路，设为$v_1v_2\cdots v_n$，如果v_1与v_n邻接，则定理得证。

如果v_1与v_n不邻接，假设v_1邻接于$\{v_{i_1}, v_{i_2}, \cdots, v_{i_k}\}2\leqslant i_j\leqslant n-1$，可以证明$v_n$必邻接于$v_{i_1-1}, v_{i_2-1}, \cdots, v_{i_k-1}$中之一。如果不邻接于$v_{i_1-1}, v_{i_2-1}, \cdots, v_{i_k-1}$中任一结点，则$v_n$至多邻接于$n-k-1$个结点，因而

$$d(v_n)\leqslant n-k-1, \quad 而 \quad d(v_1)=k$$

故$d(v_1)+d(v_n)\leqslant n-k-1+k=n-1$，与题设矛盾，所以必有汉密尔顿回路$v_1v_2\cdots v_{j-1}v_nv_{n-1}\cdots v_jv_1$，如图7-4.11所示。□

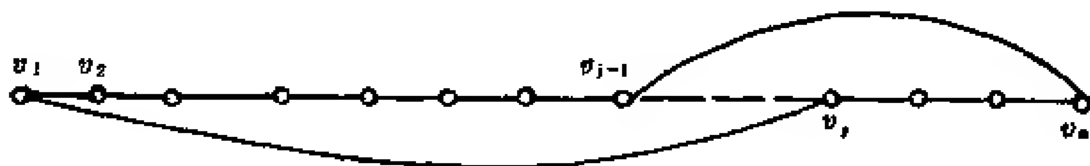


图　7-4.11

定义7-4.4　给定图$G=\langle V, E\rangle$有n个结点，若将图G中度数之和至少是n的非邻接结点连接起来得图G'，对图G'重复上述步骤，直到不再有这样的结点对存在为止，所得到的图，称为是原图G的闭包，记作$C(G)$。

例如图7-4.12给出了对六个结点的一个图G，构造它的闭包的过程。在这个例子中$C(G)$是完全图。一般情况下，$C(G)$也可能不是完全图。

定理7-4.6　当且仅当一个简单图的闭包是汉密尔顿图时，

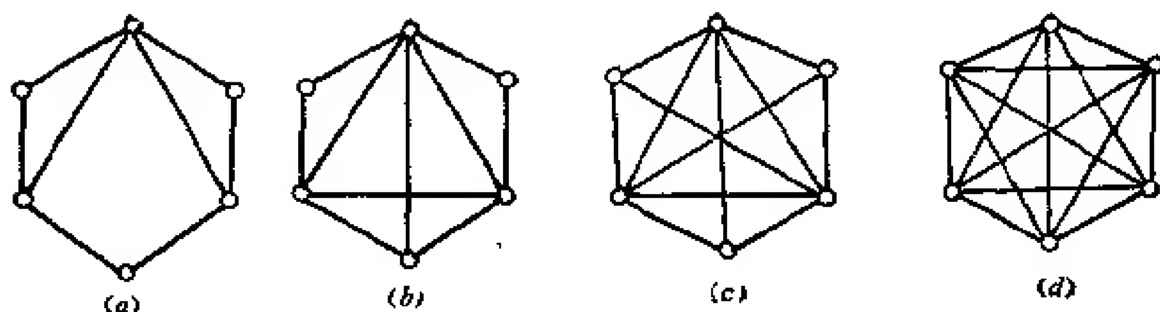


图 7-4.12

这个简单图是汉密尔顿图。

证明略。 □

关于图中没有汉密尔顿路的判别尚没有确定的方法，下面介绍一个说明性的例子。

例题2 指出图 7-4.13(a)所示的图 G 中没有汉密尔顿路。

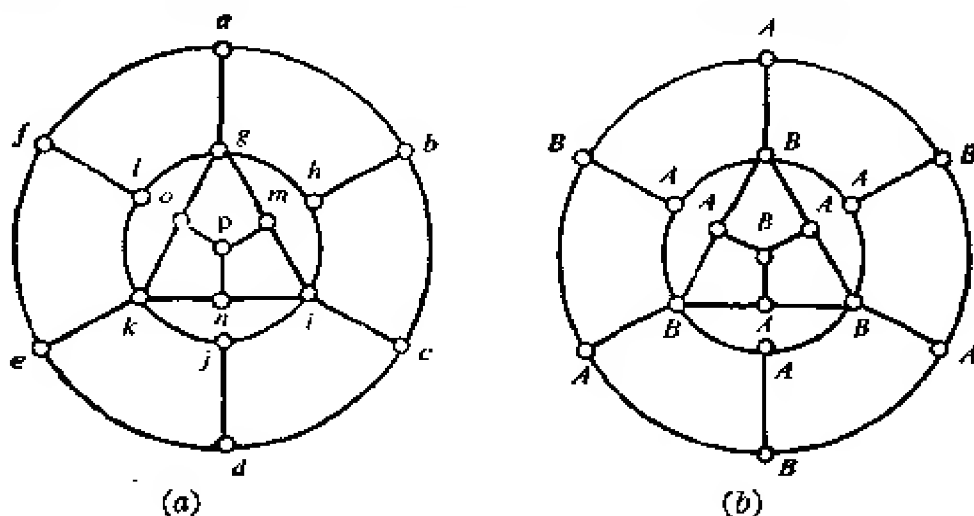


图 7-4.13

解 用 A 标记任意一个结点 a，所有与 a 邻接的结点均标记 B，继续不断地用 A 标记所有邻接于 B 的结点，用 B 标记所有邻接于 A 的结点，直到所有结点标记完毕。这个有标记的图如图7-4.13(b)所示，如果在图G中有一条汉密尔顿路，那么它必交替通过结点 A 和结点 B，然而本例中共有九个 A 结点和七个 B 结点，所以不可能存在一条汉密尔顿路。

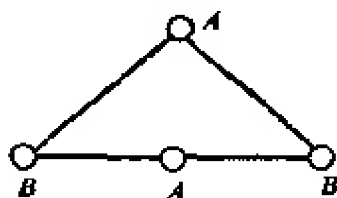
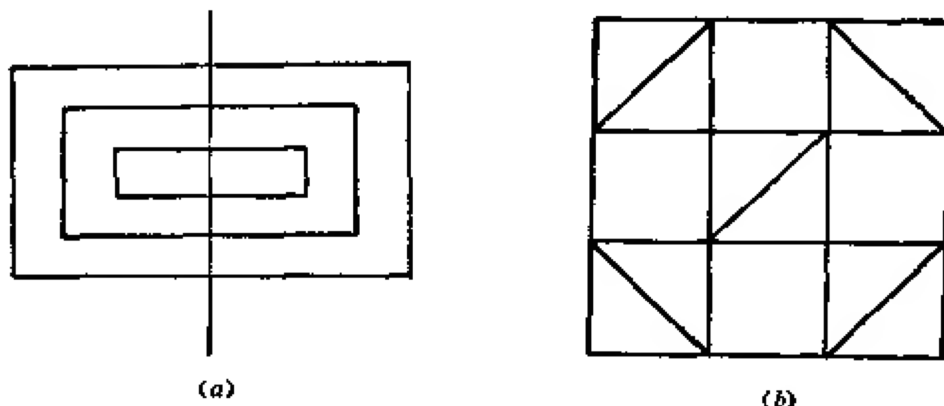


图 7-4.14

注意：如果在标记过程中，遇到相邻结点出现相同标记时，可在此对应边上增加一个结点，并标上相异标记。如图 7-4.14 所示。请读者考虑用这种方法能否判断汉密尔顿路的存在性。

7-4 习题

(1) 判定图 7-4.15 的图形是否能一笔画。



(a) (b)

图 7-4.15

(2) 构造一个欧拉图，其结点数 v 和边数 e 满足下述条件

a) v, e 的奇偶性一样。

b) v, e 的奇偶性相反。

如果不可能，说明原因。

(3) 确定 n 取怎样的值，完全图 K_n 有一条欧拉回路。

(4) a) 图 7-4.16 中的边能剖分为两条路(边不相重)，试给出这样的剖分。

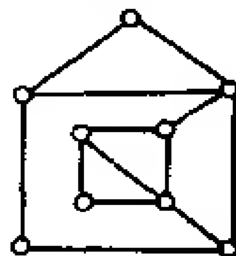


图 7-4.16

b) 设 G 是一个具有 k 个奇数度结点 ($k>0$) 的连通图，证明在 G 中的边能剖分为 $k/2$ 条路(边不相重)。

c) 设 G 是一个具有 k 个奇数度结点的图，问最少加几条边到 G 中，而使所得的图有一条欧拉回路，说明对于图 7-4.16 如何能做到这一点。

d) 在 c)中如果只允许加平行于 G 中已存在的边，问最少加几条边到 G 中，使所得的图有一条欧拉回路，这事总能做到吗？叙述能做到这事的充分必要条件。

(5) 找一种 9 个 a, 9 个 b, 9 个 c 的圆形排列，使由字母 $\{a, b, c\}$ 组成的长度为 3 的 27 个字的每个字仅出现一次。

(6) a) 画一个有一条欧拉回路和一条汉密尔顿回路的图。

b) 画一个有一条欧拉回路，但没有一条汉密尔顿回路的图。

c) 画一个没有一条欧拉回路，但有一条汉密尔顿回路的图。

(7) 判断图 7-4.17 所示的图中是否有汉密尔顿回路。

(8) 设 G 是一个具有 n 个结点的简单无向图，$n\geqslant 3$，设 G 的结点表示 n 个人，G 的边表示他们间的友好关系，若两个结点被一条边连结，当且仅当对应的人是朋友。

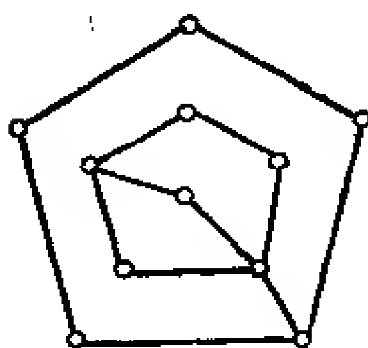


图 7-4.17

a) 结点的度数能作怎样的解释。

b) G 是连通图能作怎样的解释。

c) 假定任意两人合起来认识所留下的 $n-2$ 个人，证明 n 个人能站成一排，使得中间每个人两旁站着自己的朋友，而两端的两个人，他们每个人旁边只站着他的一个朋友。

d) 证明对于 $n\geqslant 4$，c) 中条件保证 n 个人能站成一圈，使每一个人的两旁站着自己的朋友。

(9) 证明如 G 具有汉密尔顿路，则对于 V 的每一个真子集 S 有

$$W(G-S)\leqslant |S|+1$$

(10) 一个简单图是汉密尔顿图的充要条件是其闭包是汉密尔顿图。

(11) 设简单图 $G=\langle V, E\rangle$ 且 $|V|=v$，$|E|=e$，若有 $e\geqslant C_{v-1}^{2}+2$，则 G 是汉密尔顿图。

7-5 平面图

在现实生活中，常常要画一些图形，希望边与边之间尽量减少相交的情况，例如印刷线路板上的布线，交通道的设计等。

定义 7-5.1 设 $G=\langle V, E\rangle$ 是一个无向图，如果能够把 G 的所有结点和边画在平面上，且使得任何两条边除了端点外没有其

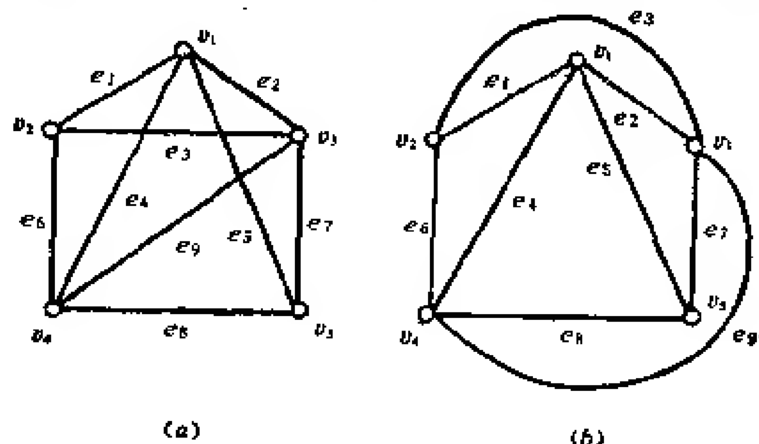


图 7-5.1

他的交点，就称 G 是一个平面图。

应该注意，有些图形从表面看有几条边是相交的，但是不能就此肯定它不是平面图，例如图 7-5.1(a)，表面看有几条边相交，但如把它画成图 7-5.1(b)，则可看出它是一个平面图。

有些图形不论怎样改画，除去结点外，总有边相交。如有三间房子 $A_1A_2A_3$，拟分别连接水、煤气和电三个接口，如图 7-5.2(a) 所示，这个图不论怎样，改画后至少有一条边与其他边相交，如图 7-5.2(b) 所示，故它是非平面图。

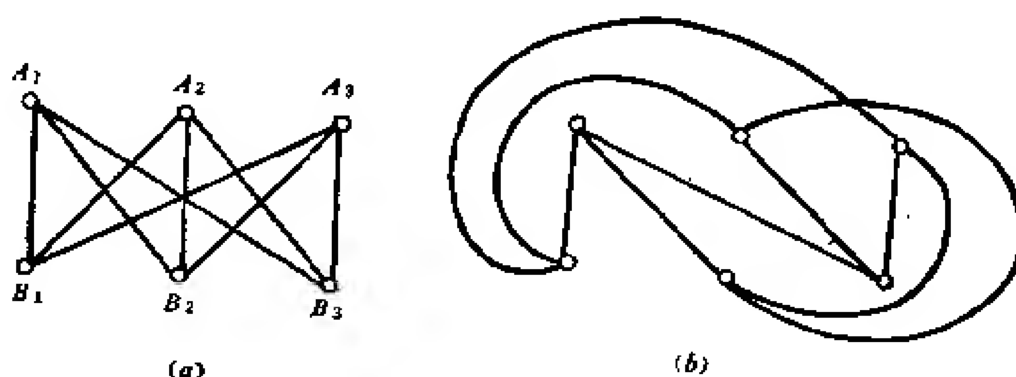


图 7-5.2

定义 7-5.2 设 G 是一连通平面图，由图中的边所包围的区域，在区域内既不包含图的结点，也不包含图的边，这样的区域称为 G 的一个面，包围该面的诸边所构成的回路称为这个面的边界。

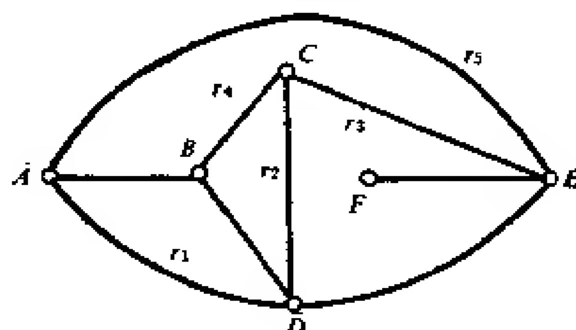


图 7-5.3

例如图 7-5.3，具有六个结点及九条边，它把平面划分为五个面。其中 r_1, r_2, r_3, r_4 四个面是由回路构成边界，如 r_1 由回路 $BADB$ 所围，r_3 可看作从 C 点开始围绕 r_3 按反时针走，得到一个回路 $CDEFEC$ 所围。另外还有一个面 r_5 在图形之外，不受边界约束，称作无限面。如果我们把图形看作包含在比整个平面还大的一个矩形之内，那么在计算图形面的数目时，就不会遗漏无限面了。今后我们把面的边界的回路长

度称作是该面的次数，记为 $\deg(r)$。如图 7-5.3 中，$\deg(r_1)=3$，$\deg(r_2)=3$，$\deg(r_3)=5$，$\deg(r_4)=4$，$\deg(r_5)=3$。

定理 7-5.1 一个有限平面图，面的次数之和等于其边数的两倍。

证明 因为任何一条边，或者是二个面的公共边，或者在一个面中作为边界被重复计算两次，故面的次数之和等于其边数的两倍。 □

如图 7-5.3 中，$\sum_{i=1}^{5}\deg(r_i)=18$，正好是边数 9 的两倍。

在三维空间中，关于凸多面体有一个著名的欧拉定理，设凸多面体有 v 个顶点 e 条棱 r 块面，则 $v-e+r=2$。我们可以把这个定理推广到平面图上来。

定理 7-5.2（欧拉定理） 设有一个连通的平面图 G，共有 v 个结点 e 条边和 r 个面，则欧拉公式

$$v-e+r=2$$

成立。

证明 (1) 若 G 为一个孤立结点，则 $v=1$，$e=0$，$r=1$，故 $v-e+r=2$ 成立。

(2) 若 G 为一条边，即 $v=2$，$e=1$，$r=1$，则 $v-e+r=2$ 成立。

(3) 设 G 为 k 条边时，欧拉公式成立。即 $v_k-e_k+r_k=2$。下面考察 G 为 $k+1$ 条边时的情况。

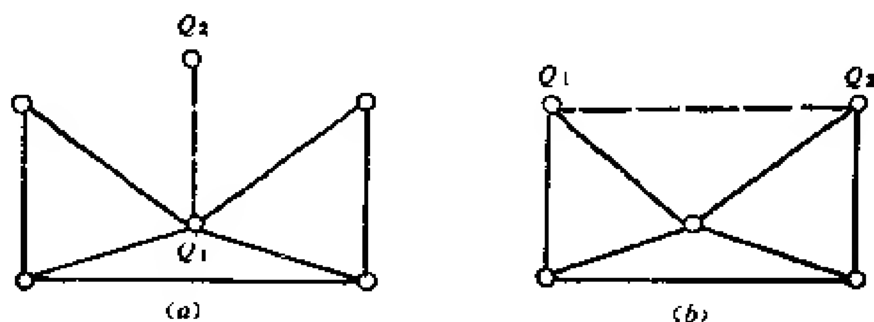


图 7-5.4

因为在 k 条边的连通图上增加一条边，使它仍为连通图，只有下述两种情况：

a) 加上一个新结点 Q_2, Q_2 与图上的一点 Q_1 相连, (如图 7-5.4(*a*) 所示), 此时 v_k 和 e_k 两者都增加1, 而面数 r_k 未变, 故

$$(v_k+1)-(e_k+1)+r_k=v_k-e_k+r_k=2$$

b) 用一条边连接图上的两已知点 Q_1 和 Q_2, 如图 7-5.4(*b*) 所示, 此时 e_k 和 r_k 都增加1而结点数 v_k 未变, 故

$$v_k-(e_k+1)+(r_k+1)=v_k-e_k+r_k=2$$ □

定理7-5.3 设 G 是一个有 v 个结点 e 条边的连通简单平面图, 若 $v\geqslant3$ 则 $e\leqslant3v-6$。

证明 设连通平面图 G 的面数为 r, 当 $v=3$, $e=2$ 时上式显然成立, 除此以外, 若 $e\geqslant3$, 则每一面的次数不小于3, 由定理 7-5.1 各面次数之和为 $2e$, 因此

$$2e\geqslant3r,\quad r\leqslant\frac{2}{3}e$$

代入欧拉定理:

$$2=v-e+r\leqslant v-e+\frac{2}{3}e$$

$$2\leqslant v-\frac{e}{3}$$

$$6\leqslant3v-e$$

$$e\leqslant3v-6$$ □

应用本定理可以判定某些图是非平面图。

例1 设图 G 如图 7-5.5 所示, 该图是 K_5 图。因为有5个结点10条边, 故 $3\times5-6<10$ 即 $3v-6\geqslant e$, 对本图不成立, 故 K_5 是非平面图。

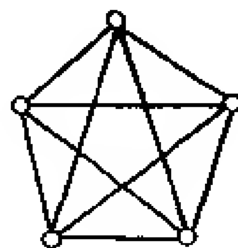


图 7-5.5

需要注意定理 7-5.3 的条件并不充分, 如图 7-5.2 中所示的图, 常称作 $K_{3,3}$ 图, 由于有6个结点9条边, 故 $3\times6-6\geqslant9$, 即满足 $3v-6\geqslant e$, 但可以证明 $K_{3,3}$ 也是非平面图。

例2 证明 $K_{3,3}$ 图不是平面图。

如果 $K_{3,3}$ 是平面图, 因为在 $K_{3,3}$ 中任取三个结点, 其中必有

两个结点不邻接，故每个面的次数都不小于 4，由 $4r \leqslant 2e$，$r \leqslant \frac{e}{2}$，即 $v-e+\frac{e}{2} \geqslant v-e+r=2$，$2v-4 \geqslant e$。在 $K_{3,3}$ 中有 6 个结点 9 条边，故 $2\times6-4<9$，即 $K_{3,3}$ 不是平面图。

虽然欧拉公式有时能用来判定某一个图是非平面图，但是还没有简便的方法可以确定某个图是平面图。下面介绍库拉托夫斯基(Kuratowski)定理。

我们可以看到在给定图 G 的边上，插入一个新的度数为 2 的结点，使一条边分成两条边，或者对于关联于一个度数为 2 的结点的两条边，去掉这个结点，使两条边化成一条边，这些都不会影响图的平面性，如图 7-5.6(*a*)与(*b*)。

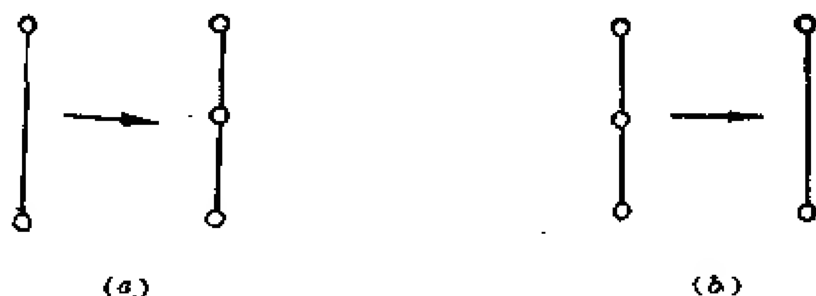


图 7-5.6

定义 7-5.3 给定两个图 G_1 和 G_2，如果它们是同构的，或者通过反复插入或除去度数为 2 的结点后，使 G_1 与 G_2 同构，则称该两图是在 2 度结点内同构的。

定理 7-5.4 (Kuratowski 定理) 一个图是平面图，当且仅当它不包含与 $K_{3,3}$ 或 K_5 在 2 度结点内同构的子图。



图 7-5.7

$K_{3,3}$ 和 K_5(如图 7-5.7) 常称作库拉托夫斯基图，这个定理虽然很基本，但证明很长，故从略。 □

7-5 习题

(1) 证明：若 G 是每一个面至少由 $k(k\geqslant 3)$ 条边围成的连通平面图，则 $e\leqslant\frac{k(v-2)}{k-2}$，这里 e，v 分别是图 G 的边数和结点数。

(2) 证明：小于 30 条边的平面简单图有一个结点度数小于等于 4。

(3) 证明：在 6 个结点 12 条边的连通平面简单图中，每个面用 3 条边围成。

(4) 设 G 是有 11 个或更多结点的图，证明 G 或 $\bar{G}$ 是非平面图。

(5) 如果可能的话，画出图 7-5.8 各图的平面图象，否则说明它包含一个与 K_5 或 $K_{3,3}$ 在 2 度结点内同构的子图。

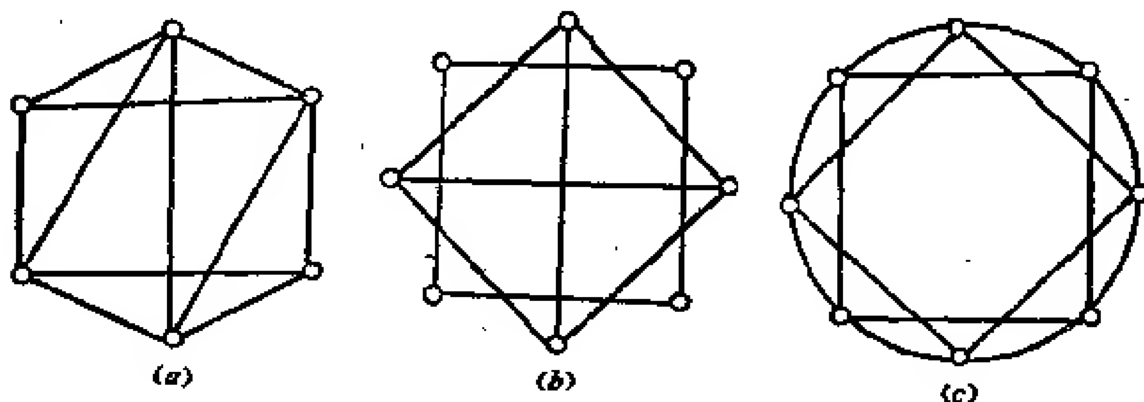


图 7-5.8

(6) 证明彼得森(Peterser)图是非平面图。(图 7-4.8)

(7) 证明：

a) 对于 K_5 的任意边 e，K_5-e 是平面图。

b) 对于 $K_{3,3}$ 的任意边 e，$K_{3,3}-e$ 是平面图。

7-6 对偶图与着色

与平面图有密切关系的一个图论的应用是图形的着色问题，这个问题最早起源于地图的着色，一个地图中相邻国家着以不同颜色，那么最少需用多少种颜色？一百多年前，英国格色里(Guthrie)提出了用四种颜色即可对地图着色的猜想，1879 年肯普(Kempe)给出了这个猜想的第一个证明，但到 1890 年希伍德(Hewood)发现肯普证明是错误的，但他指出肯普的方法，虽不能证明地图着色用四种颜色就够了，但可证明用五种颜色就够了，

此后四色猜想一直成为数学家感兴趣而未能解决的难题。直到1976年美国数学家阿佩尔和黑肯宣布：他们用电子计算机证明了四色猜想是成立的。所以从1976年以后就把四色猜想这个名词改成“四色定理”了。为了叙述图形着色的有关定理，下面先介绍对偶图的概念。

定义 7-6.1 给定平面图 $G=\langle V, E\rangle$，它具有面 $F_1, F_2, \cdots, F_n$，若有图 $G^*=\langle V^*, E^*\rangle$ 满足下述条件：

(a) 对于图 G 的任一个面 F_i，内部有且仅有一个结点 $v_i^*\in V^*$。

(b) 对于图 G 的面 F_i，F_j 的公共边界 e_k，存在且仅存在一条边 $e_k^*\in E^*$，使 $e_k^*=(v_i^*, v_j^*)$，且 e_k^* 与 e_k 相交。

(c) 当且仅当 e_k 只是一个面 F_i 的边界时，v_i^* 存在一个环 e_k^* 和 e_k 相交。则称图 G^* 是图 G 的对偶图。

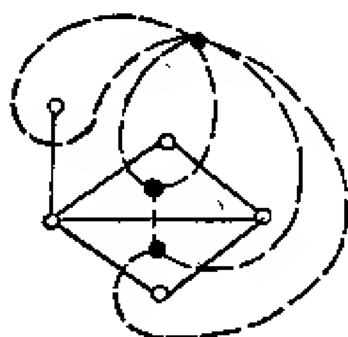


图 7-6.1

例如图 7-6.1 中，G 的边和结点分别用实线和“∘”表示。而它的对偶图 G^* 的边和结点分别用虚线和“•”表示。

从对偶图的定义，容易看到如果 G^* 是 G 的对偶图，则 G 也是 G^* 的对偶图。一个连通的平面图 G 的对偶图也必是平面图。

定义 7-6.2 如果图 G 的对偶图 G^* 同构于 G，则称 G 是自对偶图。

例如图 7-6.2 给出了一个自对偶图。

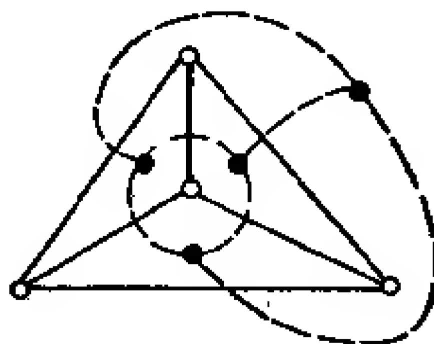


图 7-6.2

从对偶图的概念，我们可以看到，对于地图的着色问题，可以归纳为对于平面图的结点的着色问题，因此四色问题可以归结为要证明对于任何一个平面图，一定可以用四种颜色，对它的结点进行着色，使得邻接的结点都有不同的颜色。

图 G 的正常着色（或简称着色）是指对它的每一个结点指定

一种颜色，使得没有两个邻接的结点有同一种颜色。如果图 G 在着色时用了 n 种颜色，我们称 G 为 n–色的。

对于图 G 着色时，需要的最少颜色数称为 G 的着色数，记作 $x(G)$。

虽然到现在还没有一个简单的方法，可以确定任一图 G 是否是 n–色的。但我们可用韦尔奇·鲍威尔法 (Welch Powell) 对图 G 进行着色，其方法是：

a) 将图 G 中的结点按照度数的递减次序进行排列。(这种排列可能并不是唯一的，因为有些点有相同度数。)

b) 用第一种颜色对第一点着色，并且按排列次序，对与前面着色点不邻接的每一点着上同样的颜色。

c) 用第二种颜色对尚未着色的点重复 b)，用第三种颜色继续这种做法，直到所有的点全部着上色为止。

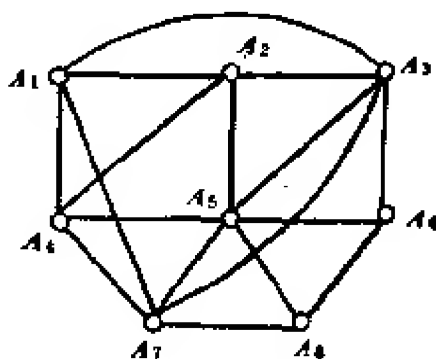


图 7-6.3

例题 1 用韦尔奇·鲍威尔法对图 7-6.3着色。

解 a) 根据递减次序排列各点 A_5, A_3, A_7, A_1, A_2, A_4, A_6, A_8。

b) 第一种颜色对 A_5 着色，并对不相邻结点 A_1 也着第一种色。

c) 对结点 A_3 和它不邻接的 A_4, A_8 着第二种颜色。

d) 对结点 A_7 和它不邻接的 A_2, A_6 着第三种颜色。

因此 G 是三色的。注意 G 不可能是二色的，因为 A_1, A_2, A_3 相互邻接，故必须着三种颜色。所以 $x(G)=3$。

定理 7-6.1 对于 n 个结点的完全图 K_n，有 $x(K_n)=n$。

证明 因为完全图的每一个结点与其他各个结点都邻接，故 n 个结点的着色数不能少于 n，又 n 个结点的着色数至多为 n，故 $x(K_n)=n$。 □

定理 7-6.2 设 G 为一个至少具有三个结点的连通平面图，则 G 中必有一个结点 u，使得 $\deg(u)\leqslant 5$。

证明 设 $G=\langle V, E\rangle$, $|V|=v$, $|E|=e$, 若 G 的每一个结

点 u，都有 $\deg(u)\geqslant 6$，但因

$$\sum_{i=1}^{v}\deg(v_i)=2e$$

故 $2e\geqslant 6v$，所以 $e\geqslant 3v>3v-6$，与定理7-5.3矛盾。 □

*定理 7-6.3　任意平面图 G 最多是5—色的。

证明　给定平面图 $G=\langle V, E\rangle$，对结点数 v 用归纳法

a) 当 $v=1, 2, 3, 4, 5$ 时显然成立。

b) 设 $v=k$ 时成立，现考察 $v=k+1$，由定理7-6.2可知，必存在结点 u，使 $\deg(u)\leqslant 5$，在图 G 中删去 u，得到 $G-\{u\}$，由归纳假设知此时定理成立。现将 u 加入到 $G-\{u\}$ 中，若 $\deg(u)<5$，则与 u 邻接的结点数不超过4，故必可对 u 正常着色，得到一个最多是五色的图 G。

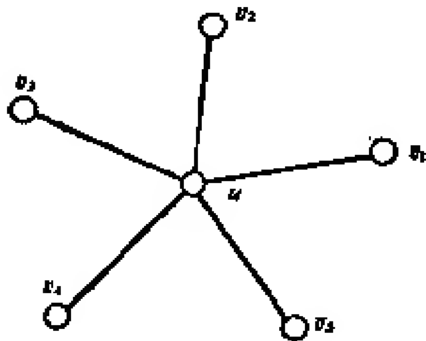


图　7-6.4

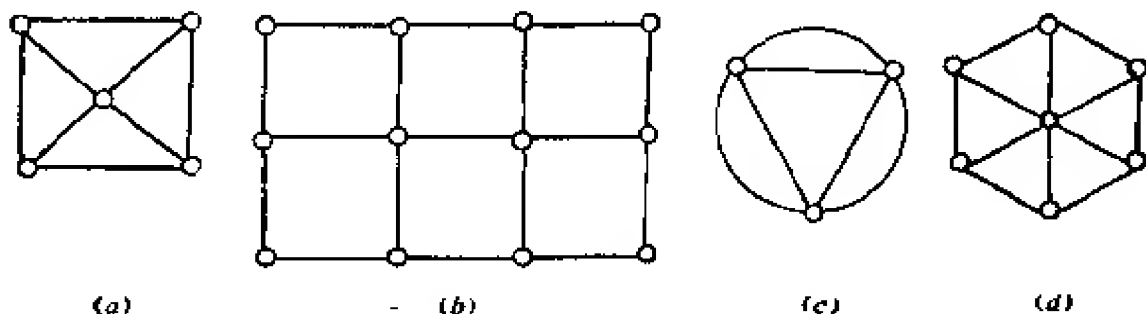
若 $\deg(u)=5$，设与 u 邻接的结点，按逆时针排列为 v_1, v_2, v_3, v_4, v_5，它们分别着不同的颜色 C_1，C_2，C_3，C_4，C_5，如图7-6.4所示。令 H 为 $G-\{u\}$ 中所有着 C_1 与 C_3 色的结点集合，F 为 $G-\{u\}$ 中着 C_2 与 C_4 的所有结点的集合。

I. 若 v_1 与 v_3 属于结点集 H 所导出子图的两个不同的连通分支中，将 v_1 所在分图中的 C_1，C_3 两种颜色对调，并不影响图 $G-\{u\}$ 的正常着色，然后在 u 上着 C_1 色，即得图 G 是五色的。

II. 若 v_1 与 v_3 属于结点集 H 所导出子图的同一个连通分支中，那么从 v_1 到 v_3 必有一条路 P，P 上的各个结点都是着 C_1 或 C_3 色。路 P 与边 (u, v_1)、(u, v_3) 一起构成了一条回路 L，它包围了 v_2 或 v_4，但不能同时包围 v_2 和 v_4，故 v_2 和 v_4 分别属于结点集 F 所导出子图的两个不同连通分支中。因此在包含 v_2 的连通分支中将 C_2 和 C_4 颜色对调并不会影响 $G-\{u\}$ 的正常着色，那样，点 v_2 与 v_4 都着了 C_4 色，故对 u 着 C_2 色，即可得到五色图 G。 □

7-6 习题

(1) 画出图 7-6.5 中各图的对偶图。

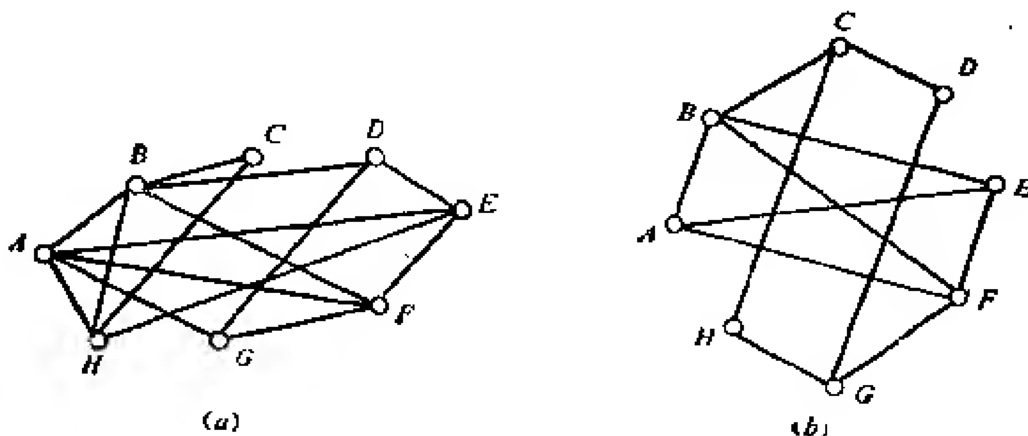


(a)　(b)　(c)　(d)

图 7-6.5

(2) 求出上题中对各图的面着色的最少色数。

(3) 用韦尔奇·鲍威尔法对图 7-6.6 各图着色，求图的着色数 n。



(a)　(b)

图 7-6.6

(4) 证明若图 G 是自对偶的，则 $e=2v-2$。

(5) 假设图 G 中各结点的度数最大为 n，证明 $x(G)\leqslant n+1$，其中 $x(G)$ 是图 G 的着色数。

(6) 证明一个无向图能被两种颜色正常着色，当且仅当它不包含长度为奇数的回路。

(7) a) 一个完全图 K_6 的边涂上红色或蓝色。证明对于任何一种随意涂边的方法，总有一个完全图 K_3 的所有边被涂上红色，或者一个 K_3 的所有边被涂上蓝色。

b) 证明六个人的人群中，或者有三个人相互认识或者有三个人彼此陌生。

c) 对于 n 个结点的完全图 K_n 的边，随意涂上红色或蓝色，证明如果有

6条或更多条红色的边关联于一个结点，则存在着一个各边都是红色的K_4或者一个蓝色的K_3。证明如果有4条或更多条蓝色的边关联于一个结点，则存在一个红色的K_4或者存在一个蓝色的K_3。

7-7 树与生成树

树是图论中重要的概念之一，它在计算机科学中应用非常广泛，这里将介绍树的一些基本性质和应用。

定义 7-7.1 一个连通且无回路的无向图称为树。树中度数为1的结点称为树叶，度数大于1的结点称为分枝点或内点。一个无回路的无向图称作森林，它的每个连通分图是树。

定理 7-7.1 给定图T，以下关于树的定义是等价的。

(1) 无回路的连通图。

(2) 无回路且$e=v-1$，其中e是边数，v是结点数。

(3) 连通且$e=v-1$。

(4) 无回路，但增加一条新边，得到一个且仅有一个回路。

(5) 连通，但删去任一边后便不连通。

(6) 每一对结点之间有一条且仅有一条路。

证明 (1)⇒(2)

设在图T中，当$v=2$时，连通无回路，T中边数$e=1$，因此$e=v-1$成立。

假设$v=k-1$时命题成立，当$v=k$时，因为无回路且连通，故至少有一条边其一个端点u的度数为1。设该边为(u, w)，删去结点u，便得到一个$k-1$个结点的连通无回路图T'，由归纳假设，图T'的边数$e'=v'-1=(k-1)-1=k-2$，于是再将结点u以及关联边(v, w)加到图T'中得到原图T，此时T的边数为$e=e'+1=(k-2)+1=k-1$，结点数$v=v'+1=(k-1)+1=k$，故$e=v-1$成立。

(2)⇒(3)

若T不连通，并且有k个连通分枝T_1, …, $T_k(k\geq 2)$因为每

个分图是连通无回路，故它们是树。设 T_i 有 v_i 个结点，这里 $v_i<v$，T_i 有 v_i-1 条边，而

$$v=v_1+v_2+\cdots+v_k$$

$$e=(v_1-1)+(v_2-1)+\cdots+(v_k-1)=v-k$$

但 $e=v-1$，故 $k=1$，这与假设 G 是不连通即 $k\geqslant 2$ 相矛盾。

(3)⇒(4)

若 T 连通且有 $v-1$ 条边。

当 $v=2$ 时，$e=v-1=1$，故 T 必无回路。如增加一边得到且仅得到一个回路。

设 $v=k-1$ 时命题成立。

考察 $v=k$ 时的情况，因为 T 是连通的，$e=v-1$。故每个结点 u 有 $\deg(u)\geqslant 1$，可以证明至少有一个结点 u_0，使 $\deg(u_0)=1$，若不然，即所有结点 u 有 $\deg(u)\geqslant 2$ 则 $2e\geqslant 2v$ 即 $e\geqslant v$，与假设 $e=v-1$ 矛盾。删去 u_0 及其关联的边，而得到新图 T'，由归纳假设可知 T' 无回路，在 T' 中加入 u_0 及其关联边又得到 T，故 T 是无回路的，若在连通图 T 中增加新的边 (u_i, u_j)，则该边与 T 中 u_i 到 u_j 的一条路构成一个回路，则该回路必是唯一的，否则若删去此新边，T 中必有回路，得出矛盾。

(4)⇒(5)

若图 T 不连通，则存在结点 u_i 与 u_j，在 u_i 与 u_j 之间没有路，显然若加边 $\{u_i, u_j\}$ 不会产生回路，与假设矛盾。又由于 T 无回路，故删去任一边，图就不连通。

(5)⇒(6)

由连通性可知，任两结点间有一条路，若存在两点，在它们之间有多于一条的路，则 T 中必有回路，删去该回路上任一条边，图仍是连通的，与(5)矛盾。

(6)⇒(1)

任意两结点间有唯一条路，则图 T 必连通，若有回路则回路上任两点间有两条路，与(6)矛盾。 □

定理 7-7.2 任一棵树中至少有两片树叶。

证明 设树 $T=\langle V, E\rangle$，$|V|=v$，因为 T 是连通图，对于任意 $v_i\in T$，有 $\deg(v_i)\geqslant 1$ 且 $\sum\deg(v_i)=2(|V|-1)=2v-2$ 若 T 中每个结点度数大于等于 2，则 $\sum\deg(v_i)\geqslant 2v$，得出矛盾。若 T 中只有一个结点度数为 1，其它结点度数大于等于 2，则

$$\sum\deg(v_i)\geqslant 2(v-1)+1=2v-1$$

得出矛盾。故 T 中至少有两个结点度数为 1。 □

有一些图，本身不是树，但它的子图却是树，一个图可能有许多子图是树，其中很重要的一类是生成树。

定义 7-7.2 若图 G 的生成子图是一棵树，则该树称为 G 的生成树。

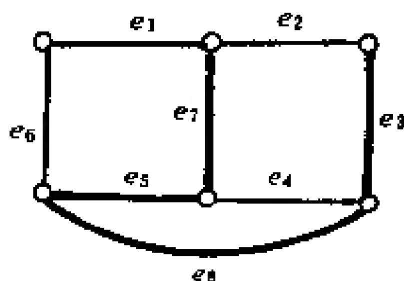


图 7-7.1

设图 G 有一棵生成树 T，则 T 中的边称作树枝。

图 G 的不在生成树中的边称作弦。所有弦的集合称作生成树 T 的补。

在图 7-7.1 中，可以看到该图的生成树 T 为粗线所表达。其中 e_1，e_7，e_5，e_8，e_3 都是 T 的树枝，e_2，e_4，e_6 是 T 的弦，$\{e_2, e_4, e_6\}$ 是生成树 T 的补。

定理 7-7.3 连通图至少有一棵生成树。

证明 设连通图 G 没有回路，则 G 本身就是一棵生成树。若 G 至少有一个回路，我们删去 G 的回路上的一条边，得到图 G_1，它仍是连通的并与 G 有同样的结点集。若 G_1 没有回路，则 G_1 就是生成树。若 G_1 仍有回路，再删去 G_1 回路上的一条边，重复上述步骤，直至得到一个连通图 H，它没有回路。但与 G 有同样的结点集，因此 H 是 G 的生成树。 □

由定理 7-7.3 的证明过程可以看出，一个连通图可以有许多生成树。因为在取定一个回路后，就可以从中去掉任一条边，去掉的边不一样，故可能得到不同的生成树。

例如在图 7-7.2(a)中，相继删去边 2、3 和 5，就得到生成树 T_1 如图 7-7.2(b)，若相继删去边 2、4 和 6，可得到生成树 T_2 如图 7-7.2(c)。

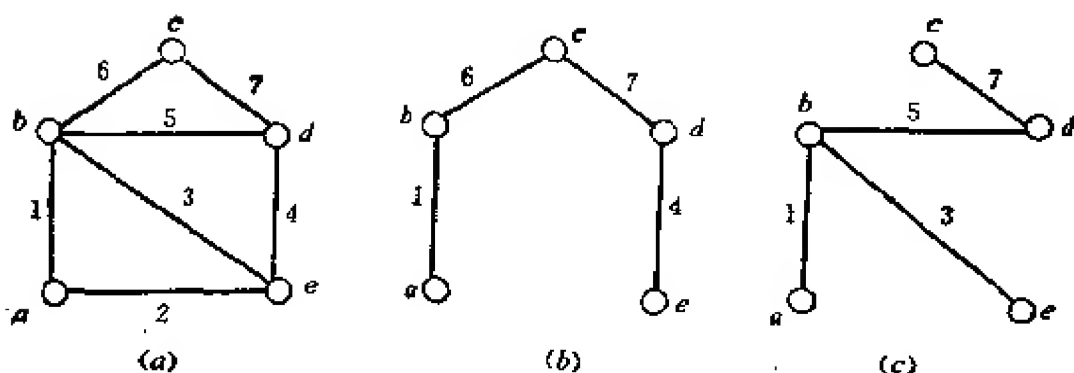


图 7-7.2

假定 G 是一个有 n 个结点和 m 条边的连通图，则 G 的生成树正好有 $n-1$ 条边。因此要确定 G 的一棵生成树，必须删去 G 的 $m-(n-1)=m-n+1$ 条边。数 $m-n+1$ 称为连通图 G 的秩。

定理 7-7.4 一条回路和任何一棵生成树的补至少有一条公共边。

证明 若有一条回路和一棵生成树的补没有公共边，那么这回路包含在生成树中，然而这是不可能的，因为一棵生成树不能包含回路。 □

定理 7-7.5 一个边割集和任何生成树至少有一条公共边。

证明 若有一个边割集和一棵生成树没有公共边，那么删去这个边割集后，所得子图必包含该生成树，这意味着删去边割集后仍是连通图，与边割集定义矛盾。 □

下面我们讨论带权的生成树。

设图 G 中结点表示一些城市，各边表示城市间道路的连接情况，边的权表示道路的长度，如果我们要用通讯线路把这些城市联系起来，要求沿道路架设线路时，所用的线路最短，这就是要求一棵生成树，使该生成树是图 G 的所有生成树中边权的和为最小。

现在讨论一般的带权图情况。

假定 G 是具有 n 个结点的连通图。对应于 G 的每一条边 e，指定一个正数 $C(e)$，把 $C(e)$ 称为边 e 的权，(可以是长度、运输量、费用等)。G 的生成树 T 也有一个树权 $C(T)$，它是 T 的所有

边权的和。

定义 7-7.3 在图 G 的所有生成树中，树权最小的那棵生成树，称作最小生成树。

定理 7-7.6(Kruskal) 设图 G 有 n 个结点，以下算法产生的是最小生成树。

a) 选取最小权边 e_1，置边数 $i \leftarrow 1$；

b) $i=n-1$ 结束，否则转 c)；

c) 设已选择边为 $e_1, e_2, \cdots, e_i$，在 G 中选取不同于 $e_1, e_2, \cdots, e_i$ 的边 e_{i+1}，使 $\{e_1, e_2, \cdots, e_i, e_{i+1}\}$ 中无回路且 e_{i+1} 是满足此条件的最小边。

d) $i \leftarrow i+1$，转 b)。

证明 设 T_0 为由上述算法构造的一个图，它的结点是图 G 的 n 个结点，T_0 的边是 $e_1, e_2, \cdots, e_{n-1}$。根据构造，$T_0$ 没有回路，由定理 7-7.1 可知 T_0 是一棵树，且为图 G 的生成树。

下面证明 T_0 是最小生成树。

设图 G 的最小生成树是 T，若 T 与 T_0 相同，则 T_0 是 G 的最小生成树。若 T 与 T_0 不同，则在 T_0 中至少有一条边 e_{i+1}，使得 e_{i+1} 不是 T 的边，但 $e_1, e_2, \cdots, e_i$ 是 T 的边。因为 T 是树，我们在 T 中加上边 e_{i+1}，必有一条回路 r，而 T_0 是树，所以 r 中必存在某个边 f 不在 T_0 中。对于树 T，若以边 e_{i+1} 置换 f，则得到新的一棵树 T'，但树 T' 的权 $C(T')=C(T)+C(e_{i+1})-C(f)$ 因为 T 是最小生成树，故 $C(T) \leqslant C(T')$ 即

$$C(e_{i+1})-C(f) \geqslant 0 \quad 或 \quad C(e_{i+1}) \geqslant C(f)$$

因为 $e_1, e_2, \cdots, e_i, f$ 是 T' 的边，且在 $\{e_1, e_2, \cdots, e_i, f\}$ 中没有回路，故 $C(e_{i+1})>C(f)$ 不可能成立，因为否则在 T_0 中，自 $e_1, e_2, \cdots, e_i$ 之后将取 f 而不能取 e_{i+1}，与题设矛盾。于是 $C(e_{i+1})=C(f)$，因此 T' 也是 G 的一棵最小生成树，但是 T' 与 T_0 的公共边比 T 与 T_0 的公共边数多 1，用 T' 置换 T，重复上面论证直至得到与 T_0 有 $n-1$ 条公共边的最小生成树，这时我们断定 T_0 是最小生成树。 □

例如图 7-7.3 中给出一个赋权连通图，粗线表示按上述算法得到的最小生成树。

以上算法中假设 G 中边权全不相同，实际上，这种算法完全适用于任意边权的情况，若有两条边权数相同，我们可以让其中的一条的权改变一个很小的量，因为 G 中边数有限，总可选择这个改变量而不影响最小生成树的最小性。

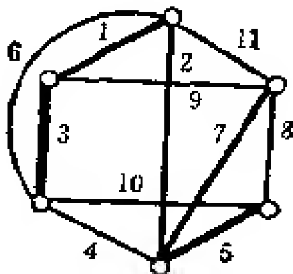


图 7-7.3

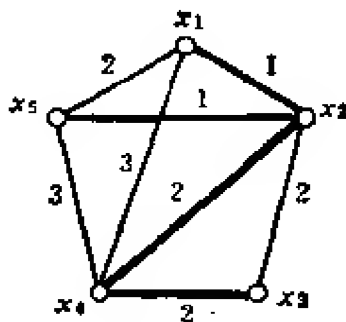


图 7-7.4

例如图 7-7.4 给出一个赋权连通图 T_0，$C(x_1,\ x_2)=1$，$C(x_2,\ x_3)=2$，$C(x_3,\ x_4)=2$，$C(x_4,\ x_5)=3$，$C(x_1,\ x_5)=2$，$C(x_2,\ x_5)=1$，$C(x_1,\ x_4)=3$，$C(x_2,\ x_4)=2$，最小生成树有边 $(x_1,\ x_2)$，$(x_2,\ x_5)$，$(x_3,\ x_4)$，$(x_2,\ x_4)$，以粗线表示。T_0 的权 $C(T_0)=6$。

7-7 习题

(1) 当且仅当连通图的每条边均为割边时，该连通图才是一棵树。

(2) 一棵树有两个结点度数为 2，一个结点度数为 3，三个结点度数为 4，问它有几个度数为 1 的结点。

(3) 一棵树有 n_2 个结点度数为 2，n_3 个结点度数为 3…，n_k 个结点度数为 k，问它有几个度数为 1 的结点。

(4) 设 T_1 和 T_2 是连通图 G 的两棵生成树，a 是在 T_1 中但不在 T_2 中的一条边，证明存在边 b，它在 T_2 中但不在 T_1 中，使得 $(T_1-\{a\})\cup\{b\}$ 和 $(T_2-\{b\})\cup\{a\}$ 都是 G 的生成树。

(5) 设 $G=\langle V,\ E\rangle$ 为连通图，且 $e\in E$。证明：当且仅当 e 是 G 的割边时，e 才在 G 的每棵生成树中。

(6) 对于图 7-7.5，利用 Kruskal 算法求一棵最小生成树。

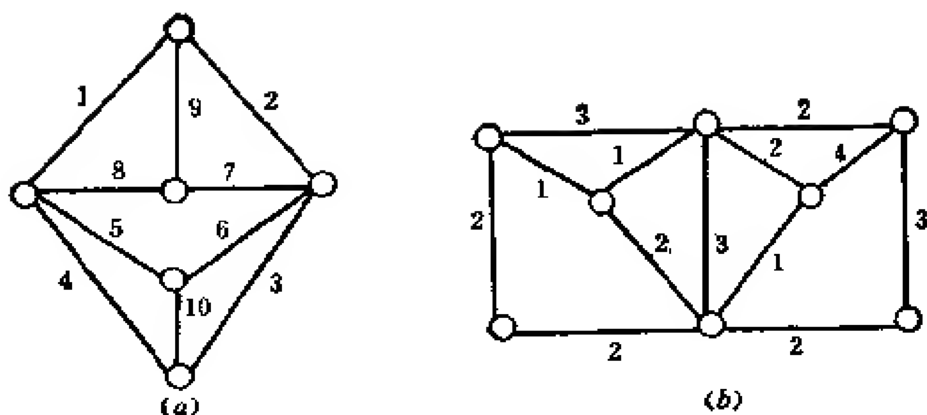


图 7-7.5

7-8 根树及其应用

前面我们讨论的树,都是无向图中的树,下面我们简单地讨论有向图中的树。

定义 7-8.1 如果一个有向图在不考虑边的方向时是一棵树,那么,这个有向图称为有向树。

例如图 7-8.1 所示为一棵有向树。

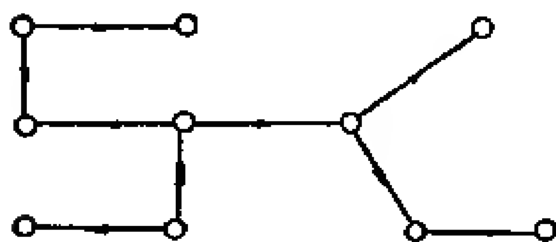


图 7-8.1

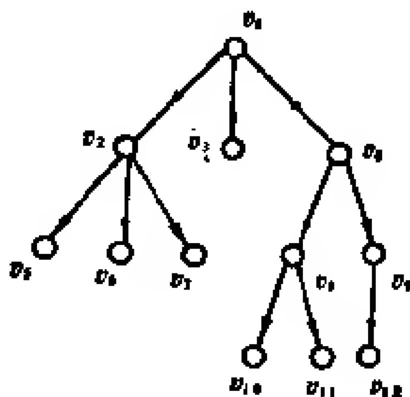


图 7-8.2

定义 7-8.2 一棵有向树, 如果恰有一个结点的入度为 0, 其余所有结点的入度都为 1, 则称为根树。入度为 0 的结点称为根, 出度为 0 的结点称为叶, 出度不为 0 的结点称为分枝点或内点。

例如图 7-8.2 表示一棵根树, 其中 v_1 为根, v_1, v_2, v_4, v_8, v_9 为分枝点, 其余结点为叶。

在根树中，任一结点 v 的层次，就是从根到该结点的单向通路长度，例如图 7-8.2 中有三个结点层次为 1，有五个结点层次为 2，有三个结点层次为 3。

从根树的结构中还可以看到，树中每一个结点都可看作是原来树中的某一棵子树的根，由此可知，根树亦可递归定义为：

定义 7-8.3 根树包含一个或多个结点，这些结点中某一个称为根，其他所有结点被分成有限个子根树。

这个定义把 n 个结点的根树用结点数少于 n 的根树来定义，最后得到每一棵都是一个结点的根树，它们就是原来那棵树的叶。

对于一棵根树，可以有树根在下或树根在上的两种不同画法，如图 7-8.3 所示。

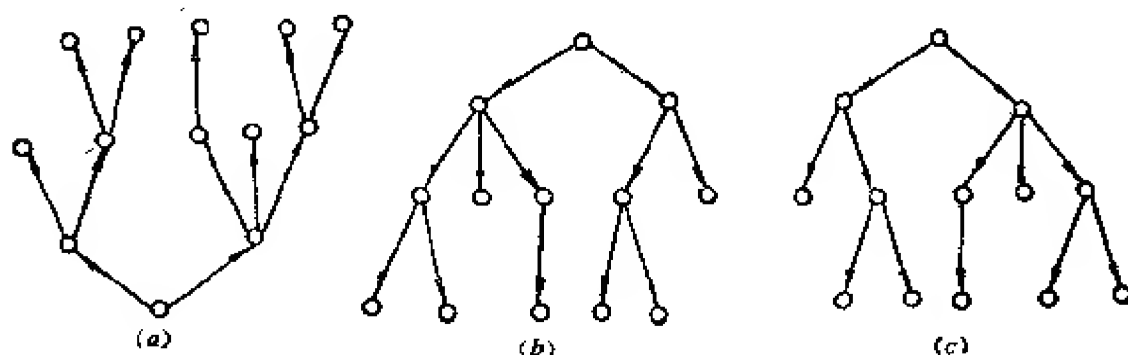


图 7-8.3

图 7-8.3(a) 是根树的自然表示法，即树从它的根向上生长。图 7-8.3(b) 和图 7-8.3(c) 都是由树根向下生长，它们是同构图，其差别仅在每一层上的结点从左到右出现的次序不同，为此，今后要用明确的方式，指明根树中结点或边的次序，这种树称为有序树。

设 a 是一棵根树的分枝点，假若从 a 到 b 有一条边，则结点 b 称为 a 的"儿子"，或称 a 为 b 的"父亲"。假若从 a 到 c 有一条单向通路，称 a 为 c 的"祖先"或 c 是 a 的"后裔"。同一个分枝点的"儿子"称为"兄弟"。

定义 7-8.4 在根树中，若每一个结点的出度小于或等于 m，则称这棵树为 m 叉树。如果每一个结点的出度恰好等于 m 或零，

则称这棵树为完全m叉树，若其所有树叶层次相同，称为正则m叉树。当$m=2$时，称为二叉树。

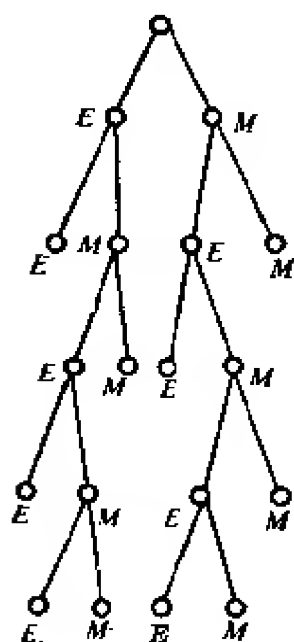


图 7-8.4

有很多实际问题可用二叉树或m叉树表示。

例如M和E两人进行网球比赛，如果一人连胜两盘或共胜三盘就获胜，比赛结束。图7-8.4表示了比赛可能进行的各种情况，它有十片树叶，从根到树叶的每一条路对应比赛中可能发生的一种情况，即：MM, $MEMM$, $MEMEM$, $MEMEE$, MEE, EMM, $EMEMM$, $EMEME$, $EMEE$, EE。

我们要指出，任何一棵有序树都可以把它改写为一棵对应的二叉树。如图7-8.5(a)中的m叉树可用下述方法改写为二叉树。

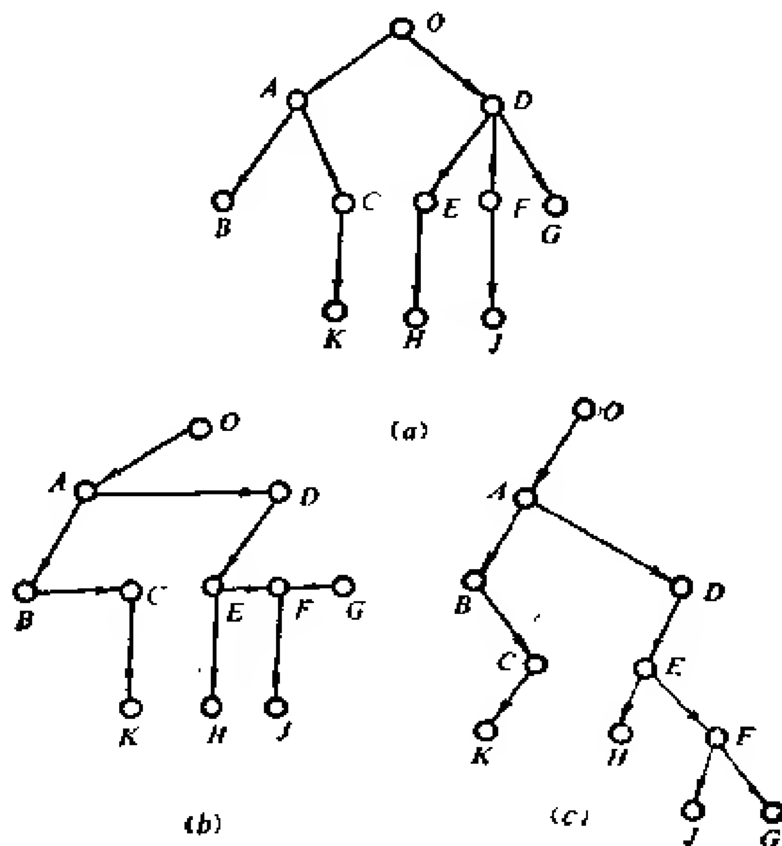


图 7-8.5

(I) 除了最左边的分枝点外，删去所有从每一个结点长出的分枝。在同一层次中，兄弟结点之间用从左到右的有向边连接，如图7-8.5 (b)所示。

(II) 选定二叉树的左儿子和右儿子如下：直接处于给定结点下面的结点，作为左儿子，对于同一水平线上与给定结点右邻的结点，作为右儿子，以此类推，如图 7-8.5(c)所示。

用二叉树表示有序根树的方法，可以推广到有序森林上去，如图 7-8.6 所示。

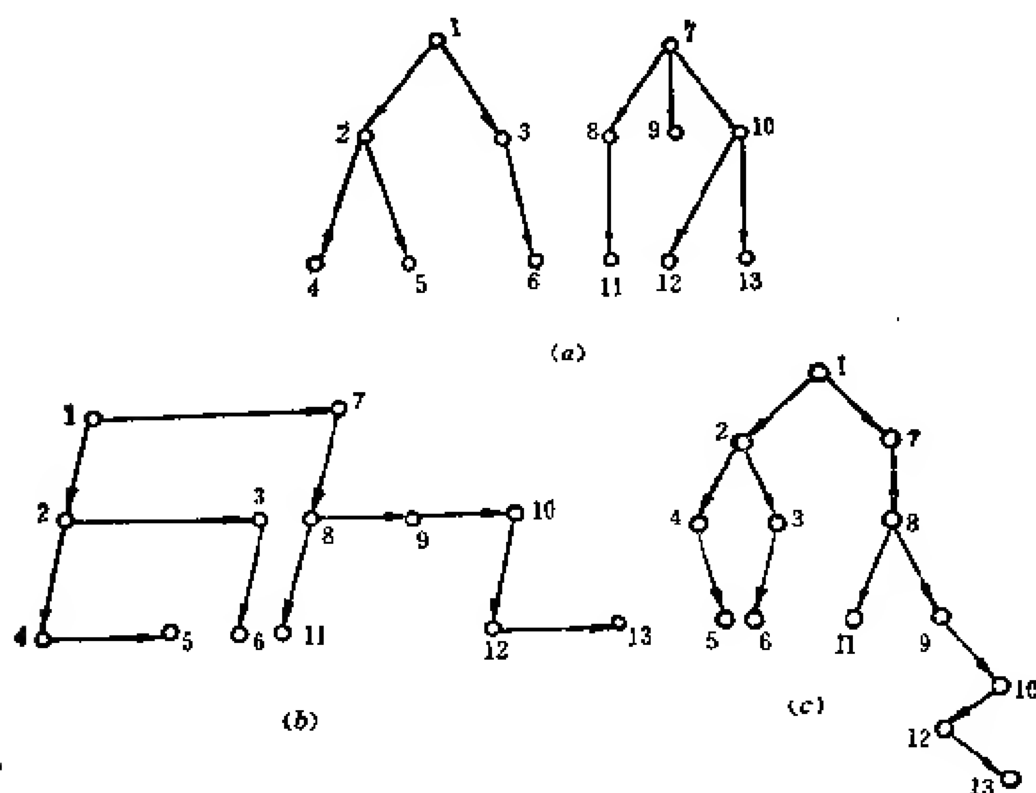


图 7-8.6

在树的实际应用中，我们经常研究完全m叉树。

定理 7-8.1 设有完全m叉树，其树叶数为t，分枝点数为i，则$(m-1)i=t-1$。

证明 若把m叉树看作是每局有m位选手参加比赛的单淘汰赛计划表，树叶数t表示参加比赛的选手数，分枝点数i表示比赛的局数，因为每局比赛将淘汰$(m-1)$位选手，故比赛结果共淘汰$(m-1)i$位选手，最后剩下一位冠军，因此$(m-1)i+1=t$，即$(m-1)i=t-1$。 □

例题1 设有28盏电灯，拟公用一个电源插座，问需用多少块具有四插座的接线板。

解 将四叉树的每个分枝点看作是具有四插座的接线板，树叶看作电灯，则有$(4-1)i=28-1$，$i=9$，所以，需要九块具有四插座的接线板。

例题2 假设有一台计算机，它有一条加法指令，可计算三个数的和，如果要计算九个数的和，至少要执行几次加法指令。

解 若把这九个数看作是完全二叉树的九片树叶，则有$(3-1)i=9-1$，$i=4$。所以，需要执行四次加法指令。

在计算机的应用中，还常常要考虑二叉树的通路长度问题。

定义7-8.5 在根树中，一个结点的通路长度，就是从树根到此结点的通路中的边数。我们把分枝点的通路长度称为内部通路长度，树叶的通路长度称为外部通路长度。

定理7-8.2 若完全二叉树有n个分枝点，且内部通路长度的总和为I，外部通路长度的总和为E，则

$$E=I+2n$$

证明 对分枝点数目n进行归纳。

当$n=1$时，$E=2$，$I=0$，故$E=I+2n$成立。

假设$n=k-1$时成立，即$E'=I'+2(k-1)$。

当$n=k$时。若删去一个分枝点v，该分枝点与根的通路长度为l，且v的两个儿子是树叶，得到新树T'。将T'与原树比较，它减少了二片长度为$l+1$的树叶和一个长度为l的分枝点，因为T'有$(k-1)$个分枝点，故$E'=I'+2(k-1)$。但在原树中，有$E=E'+2(l+1)-l=E'+l+2$，$I=I'+l$，代入上式得$E-l-2=I-l+2(k-1)$，即$E=I+2k$。 □

二叉树的一个重要应用就是最优树问题。

给定一组权$w_1, w_2, \cdots, w_t$，不妨设$w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$。设有一棵二叉树，共有$t$片树叶，分别带权$w_1, w_2, \cdots, w_t$，该二叉树称为带权二叉树。

定义7-8.6 在带权二叉树中，若带权为w_i的树叶，其通路长度为$L(w_i)$，我们把$w(T)=\sum_{i=1}^{t} w_i L(w_i)$称为该带权二叉树的

权。在所有带权 $w_1, w_2, \cdots, w_t$ 的二叉树中，$w(T)$ 最小的那棵树，称为最优树。

假若给定了一组权 $w_1, w_2, \cdots, w_t$，为了找最优树，我们先证明下面定理：

定理 7-8.3 设 T 为带权 $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$ 的最优树，则

a) 带权 w_1, w_2 的树叶 v_{w_1}, v_{w_2} 是兄弟。

b) 以树叶 v_{w_1}, v_{w_2} 为儿子的分枝点，其通路长度最长。

证明 设在带权 $w_1, w_2, \cdots, w_t$ 的最优树中，v 是通路长度最长的分枝点，v 的儿子分别带权 w_x 和 w_y，故有

$$L(w_x) \geqslant L(w_1)$$
$$L(w_y) \geqslant L(w_2)$$

若 $L(w_x) > L(w_1)$，将 w_x 与 w_1 对调，得到新树 T'，则

$$\begin{aligned} w(T') - w(T) &= (L(w_x) \cdot w_1 + L(w_1) \cdot w_x) \\ &\quad - (L(w_x) \cdot w_x + L(w_1) \cdot w_1) \\ &= L(w_x)(w_1 - w_x) + L(w_1)(w_x - w_1) \\ &= (w_x - w_1)(L(w_1) - L(w_x)) < 0 \end{aligned}$$

即 $w(T') < w(T)$，与 T 是最优树的假定矛盾。故 $L(w_x) = L(w_1)$。

同理可证 $L(w_x) = L(w_2)$。因此

$$L(w_1) = L(w_2) = L(w_x) = L(w_y)$$

分别将 w_1, w_2 与 w_x, w_y 对调得到一棵最优树，其中带权 w_1 和 w_2 的树叶是兄弟。 □

定理 7-8.4 设 T 为带权 $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$ 的最优树，若将以带权 w_1 和 w_2 的树叶为儿子的分枝点改为带权 $w_1 + w_2$ 的树叶，得到一棵新树 T'，则 T' 也是最优树。

证明 根据题设，有

$$w(T) = w(T') + w_1 + w_2。$$

若 T' 不是最优树，则必有另一棵带权 $w_1 + w_2, w_3, \cdots, w_t$ 的最优树 T''。对 T'' 中带权 $w_1 + w_2$ 的树叶 $v_{w_1+w_2}$ 生成两个儿子，得到新树 $\hat{T}$，则

$$w(\hat{T}) = w(T'') + w_1 + w_2。$$

因为 T'' 是带权 $w_1+w_2, w_3, \cdots, w_t$ 的最优树，故

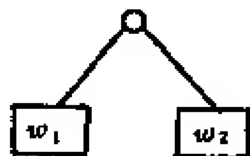
$$w(T'')\leqslant w(T')。$$

如果 $w(T'')<w(T')$，则 $w(\hat{T})<w(T)$，与 T 是带权 $w_1, w_2, \cdots, w_t$ 最优树的假设矛盾，因此，

$$w(T'')=w(T'),$$

T' 是带权 $w_1+w_2, w_3, \cdots, w_t$ 的最优树。 □

根据上述两条定理，要画一棵带有 t 个权的最优树，可简化为画一棵带有 $t-1$ 个权的最优树，而这又可简化为画一棵带有 $t-2$ 个权的最优树，依此类推。具体做法是：首先找出两个最小的 w 值，设为 w_1 和 w_2，然后对 $t-1$ 个权 $w_1+w_2, w_3, \cdots, w_t$ 求作一棵最优树，并且将这棵最优树中的结点 $\boxed{w_1+w_2}$ 代之以



依此类推。

例题 8 设有一组权2、3、5、7、11、13、17、19、23、29、31、37、41。求相应的最优树。

解 首先组合 2+3，并寻找5、5、7、11、…、41 的最优树；然后组合 5+5，依此类推。这个过程综合为：

2	**3**	5	7	11	13	17	19	23	29	31	37	41
	5	**5**	7	11	13	17	19	23	29	31	37	41
		10	**7**	11	13	17	19	23	29	31	37	41
			17	**11**	**13**	17	19	23	29	31	37	41
			17		24	**17**	19	23	29	31	37	41
					24	34	**19**	**23**	29	31	37	41
					24	34		42	**29**	31	37	41
						34		42	53	**31**	37	41
								42	53	65	**37**	**41**
								42	**53**	65		78
									95	**65**		**78**
									95			**143**
												238

它对应的最优树如图 7-8.7 所示。

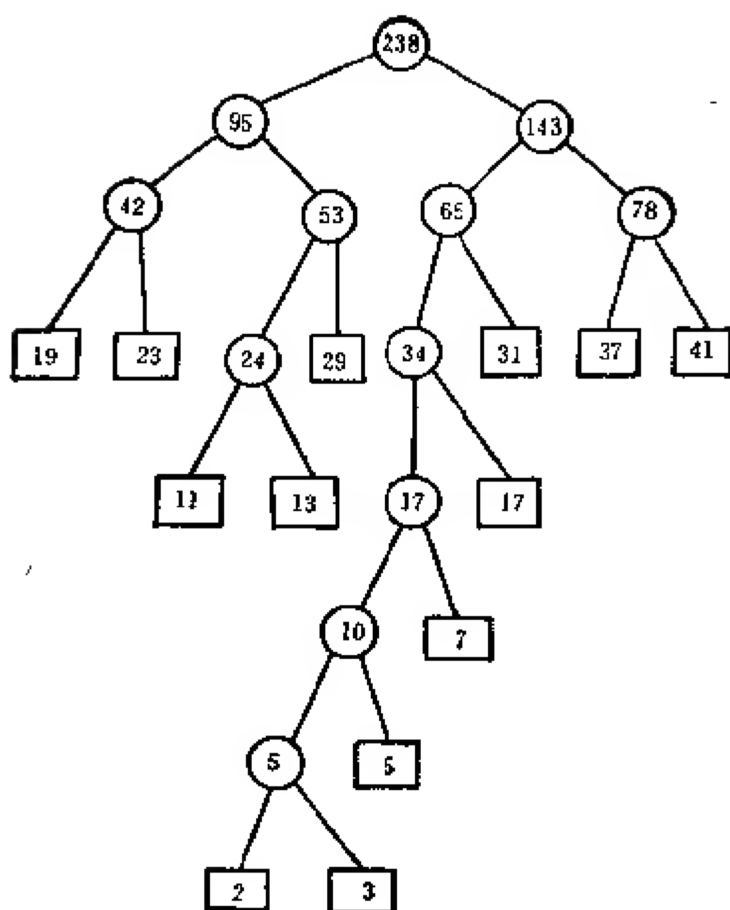


图 7-8.7

二叉树的另一个应用，就是前缀码问题。

我们知道，在远距离通讯中，常常用 0 和 1 的字符串作为英文字母的传送信息，因为英文字母共有 26 个，故如用不等长的二进制序列表示 26 个英文字母时，由于长度为 1 的序列有 2 个，长度为 2 的二进制序列有 2^2 个，长度为 3 的有 2^3 个，依此类推，我们有

$$2+2^2+\cdots+2^i\geqslant 26$$

$$2^{i+1}-2\geqslant 26,\ i\geqslant 4$$

因此，用长度不超过四的二进制序列就可表达 26 个不同英文字母。但是由于字母使用的频繁程度不同，为了减少信息量，人们希望用较短的序列去表示频繁使用的字母。当使用不同长度的序列表示字母时，我们要考虑的另一个问题是如何对接收到的字符串进行译码？

定义 7-8.7 给定一个序列的集合，若没有一个序列是另一个序列的前缀，该序列集合称为前缀码。

例如{000, 001, 01, 10, 11}是前缀码，而{1, 0001, 000}就不是前缀码。

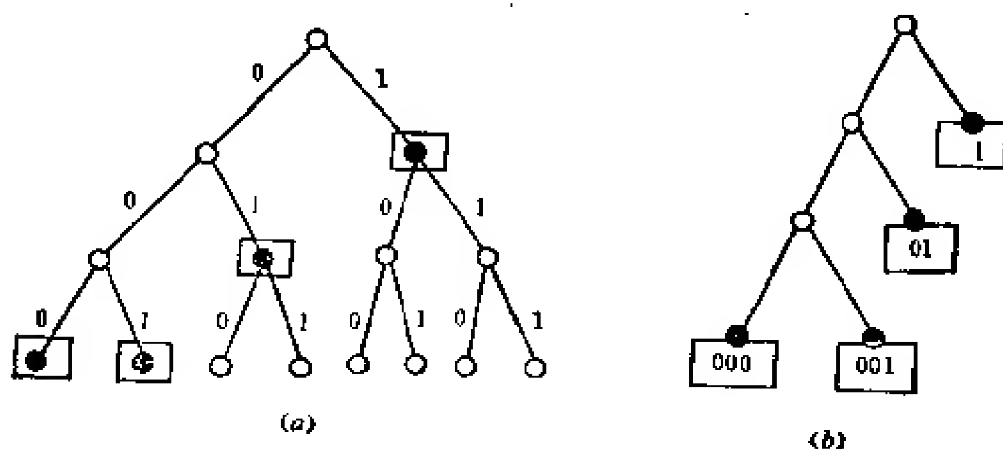
定理 7-8.5 任意一棵二叉树的树叶可对应一个前缀码。

证明 给定一棵二叉树，从每一个分枝点引出两条边，对左侧边标以 0，对右侧边标以 1，则每片树叶将可标定一个 0 和 1 的序列，它是由树根到这片树叶的通路上各边标号所组成的序列，显然，没有一片树叶的标定序列是另一片树叶标定序列的前缀，因此，任何一棵二叉树的树叶可对应一个前缀码。 □

定理 7-8.6 任何一个前缀码都对应一棵二叉树。

证明 设给定一个前缀码，h 表示前缀码中最长序列的长度。我们画出一棵高度为 h 的正则二叉树，并给每一分枝点射出的两条边标以 0 和 1，这样，每个结点可以标定一个二进制序列，它是由树根到该结点通路上各边的标号所确定，因此，对于长度不超过 h 的每一二进制序列必对应一个结点。对应于前缀码中的每一序列的结点，给予一个标记，并将标记结点的所有后裔和射出的边全部删去，这样得到一棵二叉树，再删去其中未加标记的树叶，得到一棵新的二叉树，它的树叶就对应给定的前缀码。 □

例如图 7-8.8 给出了与前缀码{000, 001, 01, 1}对应的完全二叉树，其中图(a)是高度为 3 的正则二叉树，对应前缀码中序



(a) (b)

图 7-8.8

列的结点用方框标记，图(b)是经删剪后得到的对应二叉树。

通过前缀码和二叉树的对应关系，我们可知，如果给定前缀码对应的二叉树是完全二叉树，则此前缀码可进行译码。

例如图 7-8.8(b) 中所对应的前缀码 {000, 001, 01, 1}，可对任意二进制序列进行译码。设有二进制序列 00010011011101001 可译为 000, 1, 001, 1, 01, 1, 1, 01, 001。

如果被译的信息最后部分不能成为前缀码中的序列，可约定添加 0 或 1，直至能够译出为止。

7-8 习题

(1) 从简单有向图的邻接矩阵怎样去决定它是否为根树。如果是根树，怎样定出它的树根和树叶。

(2) 求出对应于图 7-8.9 所给出的树的二叉树。

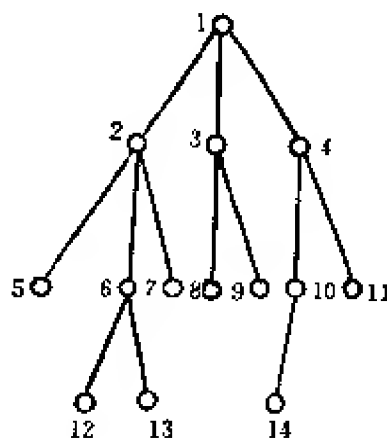


图 7-8.9

(3) 证明在完全二叉树中，边的总数等于 $2(n_t-1)$，式中 n_t 是树叶数。

(4) 在一棵 t 叉树中，其外部通路长度与内部通路长度之间有什么关系。

(5) 给定权 1, 4, 9, 16, 25, 36, 49, 64, 81, 100

a) 构造一棵最优二叉树。

b) 构造一棵最优三叉树。

c) 说明如何构造一棵最优 t 叉树。

(6) 构造一个与英文字母 b, d, g, o, y, e 对应的前缀码，并画出该前缀码对应的二叉树，再用此六个字母构成一个英文短语，写出此短语的编码信息。

(7) 设 A 是二进制序列的集合。我们将 A 划分成两个子集 A_0 和 A_1，这里 A_0 是 A 中第一个数字是 0 的序列的集合，A_1 是 A 中第一个数字是 1 的序列的集合。然后我们根据序列中的第二个数字将 A_0 划分成两个子集，对 A_1 也用同样方法加以划分。运用不断地将序列的集合划分成子集的方法来证明：如果 A 是前缀码，则存在一棵二叉树，其中从每个分枝点射出的两条边分别标号 0 和 1，使得赋于树叶的 0 和 1 的序列是 A 中的序列。

(8) 给出公式 $(P\vee(\neg P\wedge Q))\wedge((\neg P\vee Q)\wedge\neg R)$ 的根树表示。

第五篇　计算机科学中的应用

离散数学所涉及的各个课题，已在数据结构、形式语言与自动机理论、可计算理论、编码、容错诊断、人工智能、算法分析等各个领域得到广泛应用。本篇就形式语言与自动机，编码这两个专题作一个概要介绍。

第八章　形式语言与自动机

自动机的概念在1936年首先由图灵(A. M. Turing)提出，他设计的自动机称为图灵机。以后，丘奇(Church)提出了一个假设：图灵机的计算能力代表着可实现的计算装置的基本范围。可以证明，任何能在电子计算机上实现的计算都能用图灵机进行描述。

形式语言大约于1956年问世，N·乔姆斯基(Noam Chomsky)给出一种文法的数学模型。到了1959年，乔欧斯基又将文法分为四类，即0型(无限止)文法、1型(上下文有关)文法、2型(上下文无关)文法和3型(正则)文法。现在已可以证明，它们分别和图灵机、不确定的线性界限自动机、不确定的下推自动机和有限自动机等价。随着计算机高极语言的发展，人们发现ALGOL语言可由上下文无关语言定义。因此，形式语言与编译理论有着密切的联系。此外，形式语言作为一个广泛的数学模型，它描述了科学技术和各种工程中的变化过程。从此之后，研究工作相当活跃，形式语言和自动机理论相互渗透，紧密结合，使它成为计算机科学的一个重要分支。

这些理论在编译程序理论、人工智能、可计算性和时序电路设计等领域中有着广泛的应用。

本章主要介绍最简单的形式语言——正则语言以及有限自动机，给出化简有限自动机的方法。

8-1 串和语言

自然语言，例如英语，其任一单词和任一句子都是由26个英文字母和一些必要的符号连接而成，如：A language might be a given sequence of 0's and 1's.

字符串(串)就是"单词","句子"的抽象。

定义 8-1.1 任意个符号组成的集合称为字母表。字母表中的元素称为字母。一般用大写英文字母表示字母表，用小写英文字母表示字母。字母表可以是无限集，这里只考虑有限集。

定义 8-1.2 由字母表 V 中有限个字母组成的序列称为字母表 V 上的串(行)。常用小写希腊字母表示串，串 ω 中所含的字母个数称为串的长度，记作 $|\omega|$。

例如，$\omega=a_1a_2\cdots a_k$, $a_i\in V$, $1\leqslant i\leqslant k$, 是 V 上的串，且 $|\omega|=k$。

不含任何字母的串称为空串，记作 λ, 它的长度 $|\lambda|=0$。

例 1 大写英文字母表 $V_1=\{A, B, C, \cdots, Z\}$, 小写英文字母表 $V_2=\{a, b, c, \cdots, z\}$, 二进制字母表 $V_3=\{0, 1\}$ 及符号集 $V_4=\{\triangle, \odot, *, \cdots, \#\}$ 都是字母表。computer 是 V_2 上的串，长度是 8。1100100010 是 V_3 上的串，长度是 10。λ 是任一字母表上长度为 0 的唯一串。

给定字母表 V, 我们曾将笛卡尔积 $\overbrace{V\times V\times\cdots\times V}^{k}$ 记为 V^k。显然

$$V^k=\{\langle v_1, v_2, \cdots, v_k\rangle \mid v_i\in V, 1\leqslant i\leqslant k\}$$

令 $\omega=v_1v_2\cdots v_k$, ω 是 V 上长度为 k 的串，因此，V^k 中每一元素与一个长度为 k 的串一一对应，这样，就可用 V^k 表示所有长度为 k 的串组成的集合，即

$$V^k=\{\omega \mid |\omega|=k\}$$

特别地，把 V^0 看作是只包含空串的集合，用大写希腊字母 Λ 表示。

$$\Lambda=V^0=\{\lambda\}$$

集合
$$V^+=\bigcup_{i=1}^{\infty}V^i=\{\omega \mid |\omega|\geqslant 1\}$$
是字母表 V 上所有非空串的集合。

集合
$$V^*=\bigcup_{i=0}^{\infty}V^i=\{\omega \mid |\omega|\geqslant 0\}$$
是字母表 V 上所有串的集合。

例题 1 (a) 已知 $V=\{a\}$, 求 V^+, V^*;

(b) 已知 $W=\{0, 1\}$, 求 W^0, W^1 和 W^2;

(c) 求 $\emptyset^*$ 和 $\emptyset^+$。

解 (a) $V=\{a\}$, $V^2=\{aa\}$, $V^3=\{aaa\}$, $\cdots$, $V^n=\{\overbrace{aa\cdots a}^{n}\}$

$$V^+=\{a\}\cup\{aa\}\cup\{aaa\}\cup\cdots\cup\{\overbrace{aa\cdots a}^{n}\}\cup\cdots=\{a^n \mid n\geqslant 1\}$$

$$\text{其中}\quad a^n=\overbrace{aa\cdots a}^{n}$$

$$V^*=\Lambda\cup V^+=\{a^n \mid n\geqslant 0\}\quad \text{其中}\quad a^0=\lambda$$

(b) $W^0=\{\lambda\}=\Lambda$

$W^1=\{0, 1\}$

$W^2=\{00, 01, 10, 11\}$

(c) $\emptyset^*=\Lambda\cup\emptyset\cup\emptyset^2\cup\emptyset^3\cup\cdots=\Lambda$

$\emptyset^+=\emptyset\cup\emptyset^2\cup\emptyset^3\cup\cdots=\emptyset$

对于有限字母表 V, 因为 V^0, V^1, V^2, $\cdots$, V^k 是有限集, 而 V^+, V^* 都是可列个有限集的并, 所以, 它们是可列集。

V^* 上有一个基本的二元运算——连接。

定义 8-1.3 给定代数系统 $\langle V^*, \circ\rangle$, 其中 $\circ$ 是 V^* 上的一个二元运算。对于 V^* 上的任意两个串 $\omega=u_1u_2\cdots u_m$ 和 $\varphi=v_1v_2\cdots v_n$, $\omega\circ\varphi$ 也是一个串, 它前面是 ω 的符号串, 紧接着是 φ 的符号串, 即

$$\omega\circ\varphi=u_1u_2\cdots u_m v_1v_2\cdots v_n$$

二元运算 $\circ$ 称为串的连接运算。我们可以将 $\omega\circ\varphi$ 简写为 $\omega\varphi$。ω 称为 $\omega\varphi$ 的前缀, 当 $\varphi\neq\lambda$ 时, ω 称为真前缀。φ 称为 $\omega\varphi$ 的后缀, 当 $\omega\neq\lambda$ 时, φ 称为真后缀。

定理 8-1.1 代数系统 $\langle V^*, \circ\rangle$ 是一个独异点, 且

$$|\omega\varphi|=|\omega|+|\varphi|$$

证明 a) 对任意非空串 ω, $\varphi\in V^*$, 设

$$\omega=u_1u_2\cdots u_m,\quad \varphi=v_1v_2\cdots v_n$$

那么
$$\omega\circ\varphi=u_1u_2\cdots u_m v_1v_2\cdots v_n\in V^*$$

即 V^* 关于运算 $\circ$ 是封闭的, 且 $|\omega\circ\varphi|=m-n=|\omega|+|\varphi|$。

如果 ω, φ 中有一个是空串 λ, 例如设 $\omega=\lambda$, 显然

$$\omega\circ\varphi=\lambda\circ\varphi=\varphi\in V^*$$

且
$$|\omega\circ\varphi|=|\varphi|=|\omega|+|\varphi|$$

当 $\varphi=\lambda$ 时，也有 $\omega\circ\varphi\in V^*$，$|\omega\circ\varphi|=|\omega|+|\varphi|$。

b) 对任意的 ω, φ, $\psi\in V^*$，显然，$\omega\circ(\varphi\circ\psi)=(\omega\circ\varphi)\circ\psi$，即 V^* 关于运算 $\circ$ 是可结合的。

c) 对于每一 $\omega\in V^*$，显然，$\omega\circ\lambda=\lambda\circ\omega=\omega$，因此，空串 λ 是幺元。

所以，代数系统 $\langle V^*, \circ\rangle$ 是一个独异点，此独异点是不可交换的。 □

例题 2 给定代数系统 $\langle V^*, \circ\rangle$ 和 $\langle N, +\rangle$，对于任一串 $\alpha\in V^*$，建立从 V^* 到 N 的映射 f, $f(\alpha)=|\alpha|$。证明 f 是 $\langle V^*, \circ\rangle$ 到 $\langle N, +\rangle$ 的一个满同态，且当 $|V|=1$ 时，f 是同构映射。

证明 对于 V^* 中任意两个串 α 和 β，由定理 8-1.1 可知

$$|\alpha\circ\beta|=|\alpha|+|\beta|$$

所以
$$f(\alpha\circ\beta)=|\alpha|+|\beta|=f(\alpha)+f(\beta)$$

此外，$f(\lambda)=0$，对于任一正整数 $n\in N$，如果 $a\in V$，则 $|\overbrace{aa\cdots a}^{n}|=n$，所以，$f(\overbrace{aa\cdots a}^{n})=n$，$f$ 是 $\langle V^*, \circ\rangle$ 到 $\langle N, +\rangle$ 的一个满同态。

当 $|V|=1$ 时，设 $V=\{a\}$，$f(\overbrace{aa\cdots a}^{n})=n$，$f(\lambda)=0$，$f$ 是一个双射，因此，f 是一个同构映射。

连接运算 $\circ$ 是可结合的，故而我们可用 $\omega^k=\overbrace{\omega\circ\omega\circ\cdots\circ\omega}^{k}$ 表示 ω 的 k 次重复连接。当 $k=0$ 时，定义 $\omega^0=\lambda$。

定义 8-1.4 对于 V^* 中任意一个串 $\omega=v_1v_2\cdots v_n$，称串 $v_n\cdots v_2v_1$ 为串 ω 的逆，记为 ω'。

求逆运算是一个一元运算，不难证明它有下面三条性质：

1) $\lambda'=\lambda$

2) $(\omega')'=\omega$

3) 当 $\omega=\varphi\circ\psi$ 时，$\omega'=\psi'\circ\varphi'$

一个串 ω，当 $\omega=\omega'$ 时，称为回文，例如英语中的 deed，法语中的 elle 等都是回文。

定义 8-1.5 设 V 是一个有限字母表。V^* 的任意一个子集称为 V 上的一个语言。

我们常用大写字母 L 表示语言。字母表 V 上所有语言组成的集合是 V^* 的所有子集组成的集合，即幂集 $\mathscr{P}(V^*)$，因此，V 上的一个语言 L 也是 $\mathscr{P}(V^*)$ 的一个元素，$L\in\mathscr{P}(V^*)$。因为 V^* 是可数集，故 $K[V^*]=\aleph_0$，所以，L 或是有限集或是可数集。当 $V\neq\emptyset$ 时，$K[\mathscr{P}(V^*)]=2^{\aleph_0}=\aleph$，故 V 上所有语言组成的集合是不可数集。当 $V=\emptyset$ 时，V 上的语言只有一个，即 Φ，称为空语言。

例 2 设 $V=\{a\}$ 是单字母表。那么，语言

$$L=\{a^k \mid k\geqslant 0\}$$

包含所有由 a 组成的串，即 $L=\{\lambda,\ a,\ aa,\ aaa,\ \cdots\}$。

例 3 设 $V=\{0,\ 1\}$。那么，

$$L_1=\{(01)^n \mid n\geqslant 0\}=\{\lambda,\ 01,\ 0101,\ 010101,\ \cdots\}$$

$$L_2=\{0^n1^n \mid n\geqslant 0\}=\{\lambda,\ 01,\ 0011,\ 000111,\ \cdots\}$$

$$L_3=\{0^n10^n \mid n\geqslant 0\}=\{1,\ 010,\ 00100,\ 0001000,\ \cdots\}$$

都是 V 上的语言，它们都是可数集。

因为语言是集合，所以，集合上的运算，如并、交、补、差都可作为语言的基本运算。语言是由串组成的，串的连接运算亦可推广到语言上去。

定义 8-1.6 设 L_1，L_2 是字母表 V 上的两个语言。将 L_1 中每一个串后面连接上 L_2 中的一个串，所有这种串组成的集合，称为语言 L_1 和 L_2 经连接运算 $\circ$ 而得到的语言，记为 $L_1\circ L_2$，或简写为 L_1L_2，即

$$L_1\circ L_2=\{\omega\varphi \mid \omega\in L_1\wedge\varphi\in L_1\}$$

例 4 设 $V=\{a,\ b\}$，$L_1=\{\lambda,\ a,\ ab\}$，$L_2=\{a,\ bb\}$。那么，

$$L_1\cup L_2=\{\lambda,\ a,\ ab,\ bb\}$$

$$L_1\cap L_2=\{a\}$$

$$L_1L_2=\{a,\ bb,\ aa,\ abb,\ aba,\ abbb\}$$

$$L_2L_1=\{a,\ aa,\ aab,\ bb,\ bba,\ bbab\}$$

注意，一般说来，$L_1L_2\neq L_2L_1$，即语言的连接运算是不可交换的。

定理8-1.2 设 V 是任意非空有限字母表，代数系统 $\langle\mathscr{P}(V^*),\ \circ\rangle$ 是一个独异点。

证明　它的证明类似于定理 8-1.1，$\langle\mathscr{P}(V^*),\ \circ\rangle$ 的幺元是 $\Lambda=\{\lambda\}$，其余从略。□

定理8-1.3 设 $A,\ B,\ C$ 和 D 是 V 上任意语言，那么有

(a) $A\Lambda=\Lambda A=A$

(b) 如果 $A\subseteq B,\ C\subseteq D$，那么，$AC\subseteq BD$

(c) $A(B\cup C)=AB\cup AC$

(d) $(B\cup C)A=BA\cup CA$

(e) $A(B\cap C)\subseteq AB\cap AC$

(f) $(B\cap C)A\subseteq BA\cap CA$

证明　(b) 设 $\psi\in AC$，则有 $\psi=\omega\varphi$，其中 $\omega\in A,\ \varphi\in C$。而 $A\subseteq B,\ C\subseteq D$，所以，$\omega\in B,\ \varphi\in D$，即 $\psi=\omega\varphi\in BD$，因此 $AC\subseteq BD$。

(c) 先证　$AB\cup AC\subseteq A(B\cup C)$

因为 $A\subseteq A,\ B\subseteq B\cup C,\ C\subseteq B\cup C$，由(b)可知

$$AB\subseteq A(B\cup C),\quad AC\subseteq A(B\cup C)$$

所以
$$AB\cup AC\subseteq A(B\cup C)$$

再证
$$A(B\cup C)\subseteq AB\cup AC$$

设 $\psi\in A(B\cup C)$，则有 $\psi=\omega\varphi$，其中 $\omega\in A,\ \varphi\in B\cup C$，当 $\varphi\in B$ 时，有 $\psi\in AB$；当 $\varphi\in C$ 时，有 $\psi\in AC$，所以，

$$A(B\cup C)\subseteq AB\cup AC$$

由上可知
$$A(B\cup C)=AB\cup AC$$

(a)，(d)，(e)，(f)的证明留作练习。□

我们约定
$$A\emptyset=\emptyset A=\emptyset$$

注意：空集 $\emptyset$ 和以空串 λ 为唯一元素的集合 Λ 不能混为一谈，空

集 $\emptyset$ 是一个不包含任意元素的集合，而 Λ 是以空串 λ 作为唯一元素的集合。

例 5　设 $A=\{a\}$, $B=\{ba\}$, $C=\{c, cb\}$ 是 $V=\{a, b, c\}$上的三个语言。那么，$A\cap B=\emptyset$, $C(A\cap B)=C\emptyset=\emptyset$, 而

$$CA=\{ca, cba\},\ CB=\{cba, cbba\}$$

所以

$$CA\cap CB=\{cba\}$$

因此

$$C(A\cap B)\neq CA\cap CB$$

与串的逆运算一样，我们也可定义语言的逆运算。

定义 8-1.7　设 L 是字母表 V 上的一个语言，L 中每一个串的逆组成的语言，称为语言 L 的逆，记作 L'，即

$$L'=\{\varphi'\mid\varphi\in L\}$$

当 $L=L'$ 时，L 称为镜象语言。

显然，由回文组成的语言是镜象语言，但其逆不真。例如，$L=\{01, 10\}$，L 是镜象语言，但 L 中任一串都不是回文。

语言的连接运算是可结合的，我们可用 $L^k=\overbrace{L\circ L\circ\cdots\circ L}^{k}$ 表示语言 L 的 k 次重复连接。当 $k=0$ 时，$L^0=\Lambda$。

因为字母表 V 上语言的连接运算是封闭的，所以 $L^k(k\geqslant 0)$ 仍是 V 上的语言。

$$L^*=\bigcup_{k=0}^{\infty}L^k=\Lambda\cup L\cup L^2\cup L^3\cup\cdots$$

称为 L 的 *[注]闭包。

$$L^+=\bigcup_{k=1}^{\infty}L^k=L\cup L^2\cup L^3\cup\cdots$$

称为 L 的＋闭包。

显然，L^* 与 L^+ 有下列关系

$$L^*=L^+\cup\Lambda$$

定理 8-1.4　设 A 和 B 是 V 上的语言，$n\in N$。那么有

(a)　$A^n\subseteq A^*$, $n\geqslant 0$

[注]　一元运算 * 称为 Kleene star。

(b) $A^n \subseteq A^+$, $n \geqslant 1$

(c) $A \subseteq AB^*$

(d) $A \subseteq B^*A$

(e) $(A \subseteq B) \Rightarrow (A^* \subseteq B^*)$

(f) $(A \subseteq B) \Rightarrow (A^+ \subseteq B^+)$

(g) $AA^* = A^*A = A^+$

(h) $\lambda \in A \Leftrightarrow A^+ = A^*$

(i) $(A^*)^* = A^*A^* = A^*$

(j) $(A^*)^+ = (A^+)^* = A^*$

(k) $A^*A^+ = A^+A^* = A^+$

(l) $(A^*B^*)^* = (A \cup B)^* = (A^* \cup B^*)^*$

证明 (a), (b), (c), (d)的证明都是显然的，从略。

(e) 因为 $A \subseteq B$, 所以 $A^2 \subseteq B^2$, $A^3 \subseteq B^3$, …, $A^n \subseteq B^n \cdots$, 可证 $\bigcup_{n=0}^{\infty} A^n \subseteq \bigcup_{n=0}^{\infty} B^n$, 即 $A^* \subseteq B^*$。

(f)与(e)一样可证。

(h) 因为 $A^* = A^+ \cup \{\lambda\}$, 所以

$$A^* = A^+ \Leftrightarrow \lambda \in A^+ \Leftrightarrow \lambda \in A^n \Leftrightarrow \lambda \in A$$

其中 n 是一个正整数。

(l) 证明 $(A^*B^*)^* = (A \cup B)^*$

① 先证 $(A^*B^*)^* \subseteq (A \cup B)^*$

$$A \subseteq A \cup B, \quad A^* \subseteq (A \cup B)^*$$

同理 $B^* \subseteq (A \cup B)^*$, $A^*B^* \subseteq (A \cup B)^*(A \cup B)^*$

由(i)可得 $A^*B^* \subseteq (A \cup B)^*$, $(A^*B^*)^* \subseteq ((A \cup B)^*)^*$

由(i)可知 $((A \cup B)^*)^* = (A \cup B)^*$

所以, $(A^*B^*)^* \subseteq (A \cup B)^*$

② 再证 $(A \cup B)^* \subseteq (A^*B^*)^*$

由(a)可知 $A \subseteq A^*$, 由(c)可知 $A^* \subseteq A^*B^*$, 因而 $A \subseteq A^*B^*$。同样有 $B \subseteq A^*B^*$, $A \cup B \subseteq A^*B^*$。由(e)可知

$$(A \cup B)^* \subseteq (A^*B^*)^*$$

其它证明留作习题。 □

例题 3 设 $V=\{a\}$，试找出 V 上语言 A，使 $A^+ \neq A^* - \{\lambda\}$。

解 因为 $A^* = A^+ \cup \{\lambda\}$。若 $A^+ \neq A^* - \{\lambda\}$，就有 $\lambda \in A^+$，即 $\lambda \in A$。所以，$A=\{\lambda, a\}$。此时

$$A^+ = \{a^n | n \geqslant 0\}, \ A^* = \{a^n | n \geqslant 0\}$$

而
$$A^* - \{\lambda\} = \{a^n | n \geqslant 1\} \neq A^+$$

8-1 习题

(1) 设 $V=\{a, b, c\}$，求 V^2，V^3。

(2) 给出有限字母表 V，求 $|V^k|$。

(3) 设 V 是有限字母表，$|V|=n$。建立映射

$$f: \ V^* \to N$$

其中
$$f(\lambda)=0$$

$$f(\omega \circ \alpha) = nf(\omega) + h(\alpha) \begin{cases} \omega \in V^* \\ \alpha \in V \\ h: \ V \to I_n \text{ 是一个双射函数} \end{cases}$$

证明：f 是双射函数，由此可知 V^* 是可列集。

(4) 简化下列式子

a) $A\emptyset^*$

b) $A^*\emptyset^*$

c) $A^* \cup \emptyset^*$

d) $(\emptyset \cup A)^*$

e) $(A \cup A)^*$

(5) 设 V 是字母表，L 是 V 上的一个语言。定义 V^* 上的一个关系 ～：$\alpha \sim \beta$ 当且仅当对所有 $\omega, \varphi \in V^*$，有

$$(\omega\alpha\varphi \in L) \Leftrightarrow (\omega\beta\varphi \in L)$$

证明 ～ 是一个等价关系。

(6) 证明定理 8-1.3 中未证部分。

(7) 设 $A=\{\lambda, 0\}$，$B=\{0, 1\}$。列出下列集合的所有元素：

a) A^2; b) B^3; c) AB; d) A^+; e) B^*。

(8) 设 L 是字母表 V 上的语言。证明

a) $L^m L^n = L^{m+n}$， 其中 $m, n \geqslant 0$

b) $(L^m)^n = L^{mn}$， 其中 $m, n \geqslant 0$

(9) 证明：如果 $A \neq \emptyset$，$A^2 = A$，那么 $A^* = A$。反之成立吗？

(10) 证明定理 8-1.4 中未证部分。

(11) 证明：如果 L 是镜象语言，那么，L' 也是镜象语言。

(12) 给定语言 L，令 $\hat{L}=L\cap L'$。如果 L 是镜象语言，$\hat{L}$ 必是镜象语言吗？反之，如果 $\hat{L}$ 是镜象语言，L 必是镜象语言吗？

8-2 形式文法

形式语言中任一句子类似于自然语言中的句子，可逐次应用文法规则构造而成。

例 1 英语中句子

Jack and Jill ran up the hill.

它由两个短语组成

〈主语〉　　〈谓语〉

Jack and Jill　　ran up the hill

该句子是应用下列规则而构成的：

1. 〈句子〉→〈主语〉〈谓语〉
2. 〈主语〉→〈名词短语〉
3. 〈名词短语〉→〈名词〉
4. 〈名词短语〉→〈名词〉〈连接词〉〈名词短语〉
5. 〈连接词〉→and
6. 〈名词〉→Jack
7. 〈名词〉→Jill
8. 〈谓语〉→〈动词〉〈前置词短语〉
9. 〈动词〉→ran
10. 〈前置词短语〉→〈前置词〉〈冠词〉〈名词〉
11. 〈前置词〉→up
12. 〈冠词〉→the
13. 〈名词〉→hill

规则 1 到 13 构成了一个文法。我们给出的句子是此文法产生的句子之一。它的结构，可由一棵树来描述，如图 8-2.1 所示。

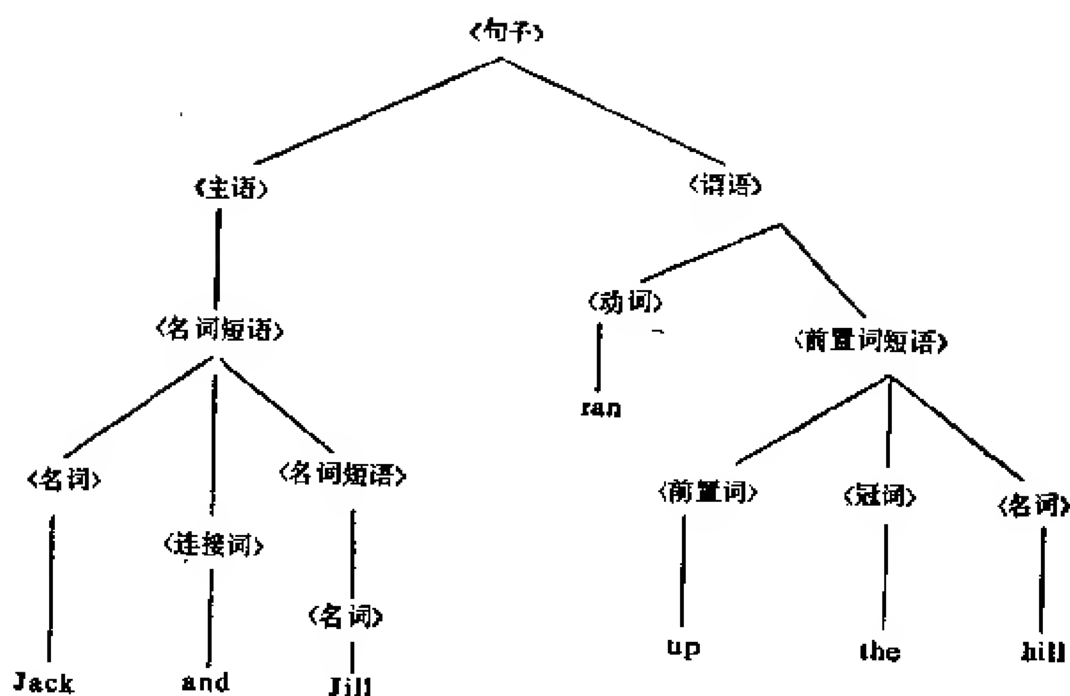


图 8-2.1

此文法也能产生

Jill and Jack ran up the hill.

Jack and Jack and Jill ran up the hill.

Hill ran up the Jack.

等句子。其中有些句子在英语中是无意义的，但在形式文法中，我们并未要求保证只生成有意义的句子。

例 2 考察 ALGOL 中的赋值语句 $x:=(1+(0+x))$ 组成此语句的字母表是 $\{x, 0, 1, +, :=, (,)\}$，它的文法规则是

1. 〈语句〉→〈左部〉〈表达式〉

   $x:=\quad(1+(0+x))$

2. 〈左部〉→〈标识符〉:=
3. 〈标识符〉→ x
4. 〈表达式〉→〈算术量〉
5. 〈算术量〉→〈项〉
6. 〈项〉→(〈表达式〉)
7. 〈算术量〉→〈项〉+〈算术量〉
8. 〈项〉→1

9. 〈项〉→0

10. 〈项〉→〈标识符〉

如果引进一些记号，S 表示〈语句〉，L 表示〈左部〉，E 表示〈表达式〉，I 表示〈标识符〉，A 表示〈算术量〉，T 表示〈项〉，那么，上述十条规则可写成

1. $S \to LE$
2. $L \to I:=$
3. $I \to x$
4. $E \to A$
5. $A \to T$
6. $T \to (E)$
7. $A \to T+A$
8. $T \to 1$
9. $T \to 0$
10. $T \to I$

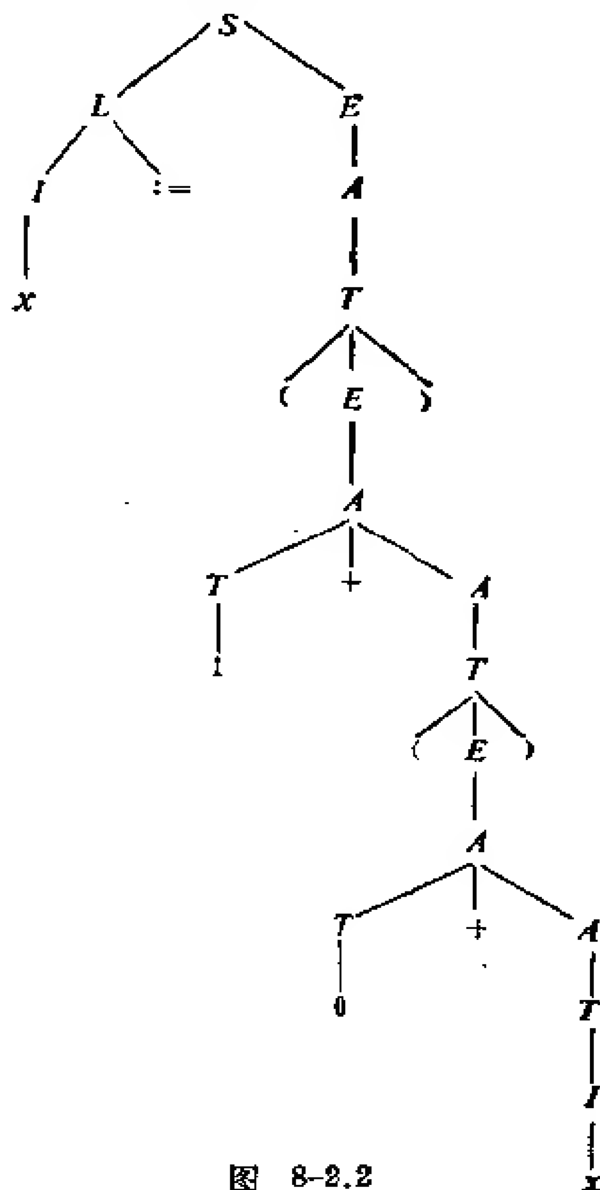


图 8-2.2

规则 1 到 10 构成了一个文法。我们给出的赋值语句是此文法产生的句子之一。它的结构，可由一棵树来描述，如图8-2.2 所示。

此文法还可产生其他赋值语句，例如 $x:=1$，$x:=x$，$x:=(0+(1+(0+(1+x))))$ 等。

从上面例子可以看到，一个文法必须要有三个主要部分：

1. 字母表：表中的字母称为终结符，因为通过文法规则，最终得到的句子只能含有这些字母，这种字母表称为终结符集。

2. 一个中间字母集，称为非终结符集。

3. 文法规则或生成式集合。

定义 8-2.1 一个形式文法是四有序组

$$G=(V_N, V_T, P, \sigma)$$

其中　V_N 是非终结符集；

V_T 是终结符集；

P 是生成式集；

σ 是开始符。

$V_N \cap V_T = \emptyset$, $\sigma \in V_N$, P 中每一生成式形为

$$\alpha \to \beta$$

其中

$$\alpha = \varphi A \psi$$

$$\beta = \varphi \omega \psi$$

φ, ψ, ω 是字母表$(V_N \cup V_T)$上的一个串，它们也可能是空串。A 是一个非终结符。

定义 8-2.2　令 $G=(V_N, V_T, P, \sigma)$。集合$(V_N \cup V_T)^*$中的符号串称为句型。如果 $\alpha \to \beta$ 是 G 的一个生成式，$\omega = \varphi\alpha\psi$ 及 $\tilde{\omega} = \varphi\beta\psi$ 是句型，称 $\tilde{\omega}$ 是 ω 的直接派生，记作 $\omega \Rightarrow \tilde{\omega}$。如果 $\omega_1, \omega_2, \cdots, \omega_n$ 是一串句型，其中 $\omega_1 \Rightarrow \omega_2 \Rightarrow \omega_3 \Rightarrow \cdots \Rightarrow \omega_n$，称 ω_n 可由 ω_1 派生得到或称 ω_n 是 ω_1 的派生，记作 $\omega_1 \overset{*}{\Rightarrow} \omega_n$。

定义 8-2.3　文法 G 生成的语言记作 $L(G)$，它是由 σ 派生得到的所有终结符串集，即

$$L(G) = \{\omega \in V_T^* \mid \sigma \overset{*}{\Rightarrow} \omega\}$$

例 3　$G_1 = (V_N, V_T, P, \sigma)$

$V_N = \{\sigma\}$, $V_T = \{0, 1\}$

P: $\sigma \to 0\sigma 1$, $\sigma \to 01$

那么　$L(G_1) = \{0^n 1^n \mid n \geq 1\}$

例 4　$G_2 = (V_N, V_T, P, \sigma)$

$V_N = \{\sigma, A\}$, $V_T = \{0, 1\}$

P: $\sigma \to 1$, $\sigma \to 1A$, $A \to 0\sigma$

那么　$L(G_2) = \{(10)^n 1 \mid n \geq 0\}$

例 5　$G_3 = (V_N, V_T, P, \sigma)$

$V_N = \{\sigma, A\}$, $V_T = \{0, 1\}$

P: $\sigma \to 1$, $\sigma \to A1$, $A \to \sigma 0$

那么

$$L(G_3) = \{1(01)^n | n \geqslant 0\} = \{(10)^n 1 | n \geqslant 0\} = L(G_2)$$

例题 1 已知 $G_4 = (V_N, V_T, P, \sigma)$, $V_N = \{\sigma, B, C\}$, $V_T = \{a, b, c\}$

P:

(1) $\sigma \to a\sigma BC$

(2) $\sigma \to aBC$

(3) $CB \to BC$

(4) $aB \to ab$

(5) $bB \to bb$

(6) $bC \to bc$

(7) $cC \to cc$

求证 $\sigma \overset{*}{\Rightarrow} a^n b^n c^n$

证明

$$\begin{aligned}
\sigma &\overset{*}{\Rightarrow} a^{n-1}\sigma(BC)^{n-1} && \text{(用生成式(1))}\\
&\Rightarrow a^n(BC)^n && \text{(用生成式(2))}\\
&\overset{*}{\Rightarrow} a^n B^n C^n && \text{(用生成式(3))}\\
&\Rightarrow a^n b B^{n-1} C^n && \text{(用生成式(4))}\\
&\overset{*}{\Rightarrow} a^n b^n C^n && \text{(用生成式(5))}\\
&\Rightarrow a^n b^n c C^{n-1} && \text{(用生成式(6))}\\
&\overset{*}{\Rightarrow} a^n b^n c^n && \text{(用生成式(7))}
\end{aligned}$$

例如 $n=3$ 的派生过程是

$$\begin{aligned}
&\sigma \Rightarrow a\sigma BC \Rightarrow a^2\sigma BCBC \Rightarrow a^3BCBCBC\\
&\Rightarrow a^3BBCCBC \Rightarrow a^3BBCBCC \Rightarrow a^3BBBCCC\\
&\Rightarrow a^3bBBCCC \Rightarrow a^3b^2BCCC \Rightarrow a^3b^3CCC\\
&\Rightarrow a^3b^3cCC \Rightarrow a^3b^3c^2C \Rightarrow a^3b^3c^3
\end{aligned}$$

例题 2 已知 $G_5 = (V_N, V_T, P, \sigma)$, $V_N = \{\sigma, A, B\}$, $V_T = \{0, 1\}$

P:

$\sigma \to 0B$	$A \to 1AA$
$\sigma \to 1A$	$B \to 1$
$A \to 0$	$B \to 1\sigma$
$A \to 0\sigma$	$B \to 0BB$

求证 $L(G_5)$是由相同个数的 0 和 1 所组成的 V_T^+ 中所有串的集合。

证明 令 $N_0(\omega)$ 表示串 ω 中 0 的个数,$N_1(\omega)$ 表示串 ω 中 1 的个数。我

们对 V_T^+ 中的 ω 长度作归纳证明。

(1) $\sigma \overset{*}{\Rightarrow} \omega$，当且仅当 $N_0(\omega)=N_1(\omega)$

(2) $A \overset{*}{\Rightarrow} \omega$，当且仅当 $N_0(\omega)=N_1(\omega)+1$

(3) $B \overset{*}{\Rightarrow} \omega$，当且仅当 $N_0(\omega)+1=N_1(\omega)$

若 $|\omega|=1$，因有 $A \Rightarrow 0$，$B \Rightarrow 1$，且从 σ 不能派生出长度为 1 的终结符串，同样，从 A 和 B 不可能派生出除 0 和 1 之外长度为 1 的串来，所以归纳基成立。

设 $|\omega| \leqslant k-1$ 时成立，当 $|\omega|=k$ 时。

(1) 若 $\sigma \overset{*}{\Rightarrow} \omega$，则派生是以 $\sigma \Rightarrow 0B$ 或 $\sigma \Rightarrow 1A$ 开始，若 $\sigma \Rightarrow 0B$，则 $\omega=0\omega_1$，$|\omega_1|=k-1$，$B \overset{*}{\Rightarrow} \omega_1$，由归纳假设可知，$N_0(\omega_1)+1=N_1(\omega_1)$，所以

$$N_0(\omega)=N_0(\omega_1)+1=N_1(\omega_1)=N_1(\omega)$$

若 $\sigma \Rightarrow 1A$，可以类似证明。

反之，若 $|\omega|=k$ 且 $N_0(\omega)=N_1(\omega)$。若 $\omega=0\omega_1$，$|\omega_1|=k-1$，$N_0(\omega_1)+1=N_1(\omega_1)$，由归纳假设有 $B \overset{*}{\Rightarrow} \omega_1$，故我们有 $\sigma \Rightarrow 0B \overset{*}{\Rightarrow} 0\omega_1=\omega$。若 $\omega=1\omega_1$，可以类似证明。

(2) 若 $A \overset{*}{\Rightarrow} \omega$，则派生是以 $A \Rightarrow 0\sigma$ 或 $A \Rightarrow 1AA$ 开始。若 $A \Rightarrow 0\sigma$，则 $\omega=0\omega_1$，$|\omega_1|=k-1$，且 $\sigma \overset{*}{\Rightarrow} \omega_1$，由归纳假设可知，$N_0(\omega_1)=N_1(\omega_1)$，所以 $N_0(\omega)=N_0(\omega_1)+1=N_1(\omega_1)+1=N_1(\omega)+1$。若 $A \Rightarrow 1AA$，则 $\omega=1\omega_1\omega_2$，$|\omega_1|<k-1$，$|\omega_2|<k-1$，且 $A \overset{*}{\Rightarrow} \omega_1$，$A^* \Rightarrow \omega_2$，由归纳假设可知，

$$N_0(\omega_1)=N_1(\omega_1)+1,\ N_0(\omega_2)=N_1(\omega_2)+1,$$

所以

$$N_0(\omega)=N_0(\omega_1)+N_0(\omega_2)=N_1(\omega_1)+1+N_1(\omega_2)+1=N_1(\omega)+1。$$

反之，若 $|\omega|=k$，且 $N_0(\omega)=N_1(\omega)+1$。若 $\omega=0\omega_1$，$|\omega_1|=k-1$，$N_0(\omega_1)=N_0(\omega)-1=N_1(\omega)=N_1(\omega_1)$，由归纳假设有 $\sigma \overset{*}{\Rightarrow} \omega_1$，故我们有 $A \Rightarrow 0\sigma \overset{*}{\Rightarrow} 0\omega_1=\omega$。

若 $\omega=1\omega_1$，$N_0(\omega_1)=N_0(\omega)=N_1(\omega)+1=N_1(\omega_1)+2$，必有 $\omega_1=\omega_2\omega_3$，$N_0(\omega_2)=N_1(\omega_2)+1$，$N_0(\omega_3)=N_1(\omega_3)+1$，$|\omega_2|<k-1$，$|\omega_3|<k-1$，由归纳假设有 $A \overset{*}{\Rightarrow} \omega_2$，$A \overset{*}{\Rightarrow} \omega_3$，故我们有 $A \Rightarrow 1AA \overset{*}{\Rightarrow} 1\omega_2A \overset{*}{\Rightarrow} 1\omega_2\omega_3=1\omega_1=\omega$。

(3)的证明与(2)类似。

从上面的讨论可知，一个文法所产生的语言，主要由生成式来决定。

下面讨论文法的分类，形式文法可以分为四类：

(A) 无限止文法(0型)

无限止文法是最普遍的一类文法，在它的生成式 $\varphi A\psi\to\varphi\omega\psi$ 中，ω 可以是 λ，因此，如果句型 β 是由句型 α 应用 $\varphi A\psi\to\varphi\lambda\psi$ 生成式而得到的派生，那么，$|\alpha|>|\beta|$，这种规则称为缩减规则，只有0型文法能缩减。由0型文法产生的语言称为0型语言。

(B) 上下文有关文法(1型)

此文法要求所有的生成式 $\varphi A\psi\to\varphi\omega\psi$ 中，$\omega\neq\lambda$，即要求所有生成式是非缩减的。因此，在1型文法中，如有

$$\omega_1\Rightarrow\omega_2\Rightarrow\cdots\Rightarrow\omega_n$$

则

$$|\omega_1|\leqslant|\omega_2|\leqslant\cdots\leqslant|\omega_n|$$

由此可知，如果 G 是上下文有关文法，$\lambda\in L(G)$ 当且仅当 G 包含 $\sigma\to\lambda$ 生成式。由1型文法产生的语言称为1型语言。

在例题1中，将生成式(3) $CB\to BC$ 改写为 $CB\to DB$，$DB\to DE$，$DE\to BE$，$BE\to BC$，那么，它就是1型文法。

(C) 上下文无关文法(2型)

此文法要求所有的生成式 $\varphi A\psi\to\varphi\omega\psi$ 中，$\varphi=\psi=\lambda$ 且 $\omega\neq\lambda$，即它的生成式形为

$$A\to\omega\quad(\omega\neq\lambda)$$

在此文法中，所有生成式左端是一个非终结符。与上下文有关文法一样，$\lambda\in L(G)$ 当且仅当 G 包含生成式 $\sigma\to\lambda$。由2型文法产生的语言称为2型语言。

上面例3和例题2中的文法都是2型文法。

(D) 正则文法(3型)

正则文法是上下文无关文法的一种特殊情况，它要求所有生成式 $A\to\omega$ 中，ω 至多含有一个非终结符。

所有生成式形为

$$A\to aB\quad 或\quad A\to a$$

其中 $A, B\in V_N$，$a\in V_T$ 的文法称为右线性文法。

所有生成式形为

$$A \to Ba \quad 或 \quad A \to a$$

其中 $A, B \in V_N$, $a \in V_T$ 的文法称为左线性文法。

右线性文法，左线性文法都是正则文法。由正则文法产生的语言称为正则语言。$\lambda \in L(G)$ 当且仅当 G 包含生成式 $\sigma \to \lambda$。

上面例 4 的文法是右线性文法，例 5 的文法是左线性文法。

以上讨论的四类文法，它们相互之间的关系可如图 8-2.3 所示。

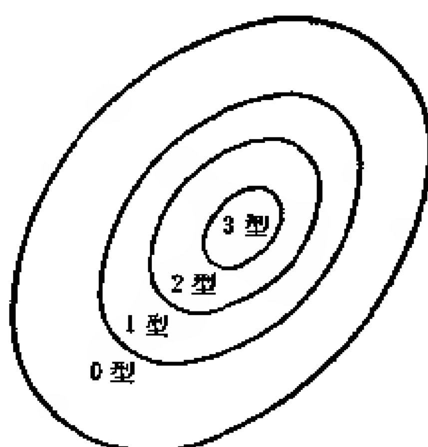


图 8-2.3

前面已经提到，可以用树将某些语言中句子的派生过程清楚地显示出来。

下面讨论上下文无关文法和正则文法的派生树。

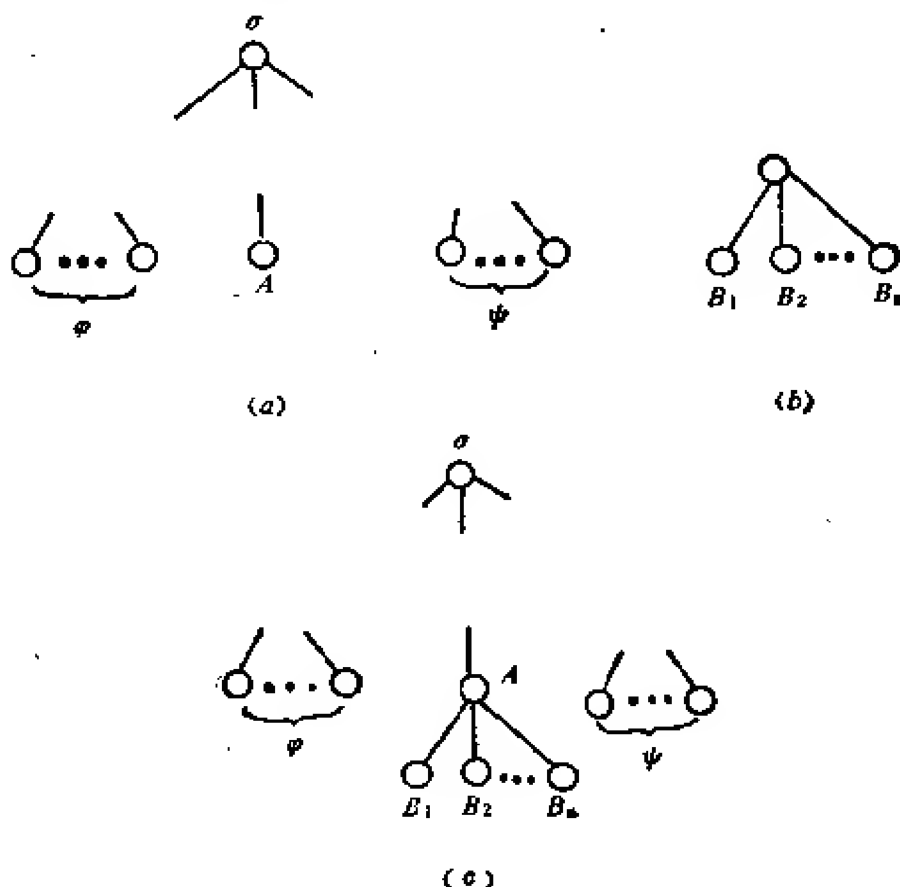


图 8-2.4

用开始符标识树根，派生过程中的非终结符标识树的分枝点，最后得到的终结符串中的字母标识树叶，这样得到的树称为派生树。派生树的构造是按照派生过程逐步得到，如果已有 $\sigma \overset{*}{\Rightarrow} \varphi A \psi$，其中 $\varphi, \psi \in (V_N \cup V_T)^*$，它的派生树如图 8-2.4($a$) 所示。接着使用生成式 $A \to B_1 B_2 \cdots B_n$，其中 $A \in V_N$，$B_i \in (V_N \cup V_T)$，$(1 \leqslant i \leqslant n)$，并用图 8-2.4($b$) 所示的子树代替标识为 A 的叶，得到新的派生树，如图 8-2.4(c) 所示。

按照这种方法构造下去，直到所有叶都是以终结符标识为止。

例题 3 给出上下文无关文法 $G=(V_N, V_T, P, \sigma)$ 其中 $V_N=\{\sigma, T\}$，$V_T=\{(,)\}$，P: $\sigma \to \sigma T$，$\sigma \to T$，$T \to (\sigma)$，$T \to (\ )$。

求 串( )(( )) 的派生过程及派生树。

解 串( )(( )) 的派生过程为：

$$\sigma \Rightarrow \sigma T \Rightarrow TT \Rightarrow (\ )T \Rightarrow (\ )(\sigma)$$
$$\Rightarrow (\ )(T) \Rightarrow (\ )((\ ))。$$

它所对应的派生树如图 8-2.5 所示。

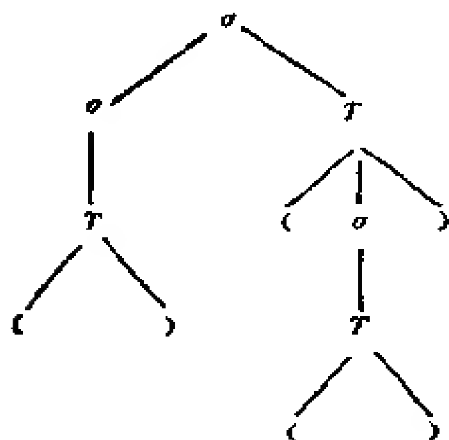


图 8-2.5

串( )(( )) 的派生过程不是唯一的，下面是它的另一派生过程：

$$\sigma \Rightarrow \sigma T \Rightarrow \sigma(\sigma) \Rightarrow \sigma(T) \Rightarrow \sigma((\ ))$$
$$\Rightarrow T((\ )) \Rightarrow (\ )((\ ))$$

它对应的派生树与图 8-2.5 相同。

对于正则文法，派生树的形式更为简单。右线性文法所对应的派生树只能在右面衍生。左线性文法所对应的派生树只能在左面衍生。

例题 4 构造例 4 和例 5 中文法所对应的派生树。

解 例 4 和例 5 分别是右线性文法和左线性文法，它们对应的派生树分别如图 8-2.6(a)和(b)所示。

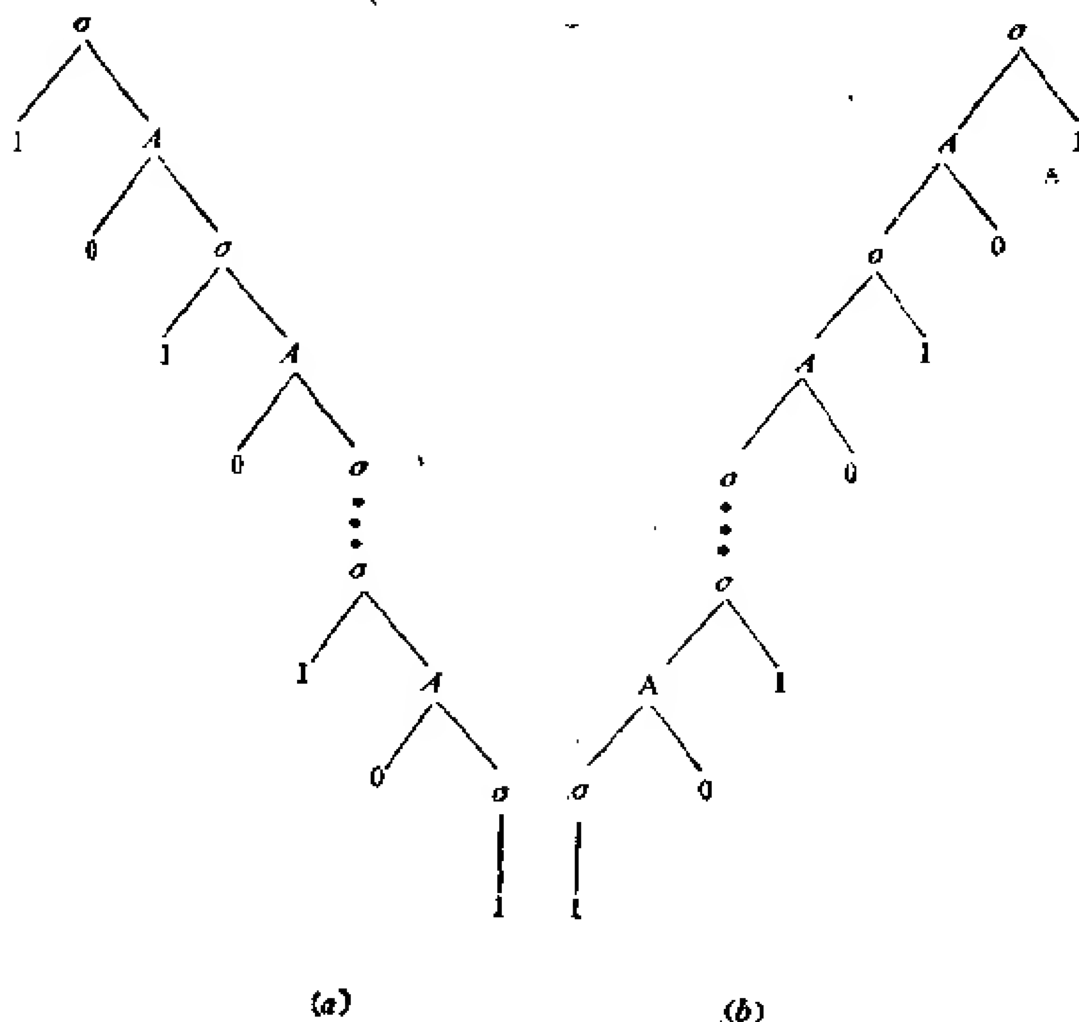


图 8-2.6

8-2 习题

(1) 给定文法 $G=(\{\sigma, A\}, \{0, 1\}, P, \sigma)$，其中

$$P:\ \sigma\to 0\sigma,\quad \sigma\to 1A,\quad \sigma\to 0$$
$$A\to 0A,\quad A\to 1\sigma,\quad A\to 1$$

描述 $L(G)$，写出 00101 的派生过程并画出派生树。

(2) 考察下列文法

$$G_1=(\{\sigma\}, \{c\}, P_1, \sigma)$$

其中 $$P_1:\ \sigma\to\lambda,\ \sigma\to\sigma\sigma,\ \sigma\to c$$

$$G_2=(\{\sigma\}, \{c\}, P_2, \sigma)$$

其中 $$P_2:\ \sigma\to\lambda,\ \sigma\to\sigma c\sigma,\ \sigma\to c$$

a) 描述 $L(G_i)(i=1, 2)$

b) 对每一语言，给出一个长度为 5 的终结符串的派生，并构造派生树。

(3) 证明串 $a^n b^n c^n$, $n\geqslant 1$ 是例题 1 中 $L(G_4)$ 中仅有的终结符串。由此

可知，$L(G_4)=\{a^n b^n c^n \mid n\geqslant 1\}$。

(4) a) 构造一个左线性文法 G，使 $L(G)=\{10^n \mid n\geqslant 0\}$；

b) 构造一个右线性文法 G，使 $L(G)=\{ab^m \mid m\geqslant 0\}\cup\{c^n \mid n\geqslant 0\}$。

(5) 设 G 为一文法，且它的所有生成式的形式都是 $A\to\varphi B$ 和 $A\to\varphi$，其中 $A, B\in V_N$，$\varphi\in V_T^*$。试证 G 产生的语言 $L(G)$ 能由右线性文法产生。

(6) 给出一个产生下列语言

$L=\{\omega \mid \omega\in\{0, 1\}^*$ 且 ω 不含有两个相邻的 $1\}$ 的正则文法。

(7) 给出一个产生下列语言 $L=\{\omega\omega' \mid \omega\in\{0, 1\}^*\}$ 的上下文有关文法。

(8) 考察下列 0 型文法：

$$G=(\{\sigma, A, B, C, D, E\}, \{0, 1\}, P, \sigma)$$

其中

$$\begin{array}{llll} P: & \sigma\to ABC & AB\to 0AD & AB\to 1AE \\ & AB\to\lambda & D0\to 0D & D1\to 1D \\ & E0\to 0E & E1\to 1E & C\to\lambda \\ & DC\to B0C & EC\to B1C & 0B\to B0 \\ & 1B\to B1 & & \end{array}$$

描述 $L(G)$，并写出 01100110 的派生过程。

8-3 有限状态自动机

上面我们用文法表示了语言，从本节起将用另一种方法——识别器来描述语言，为此，现在我们先介绍有限状态自动机。

考察一台信号转换器，如图 8-3.1 所示

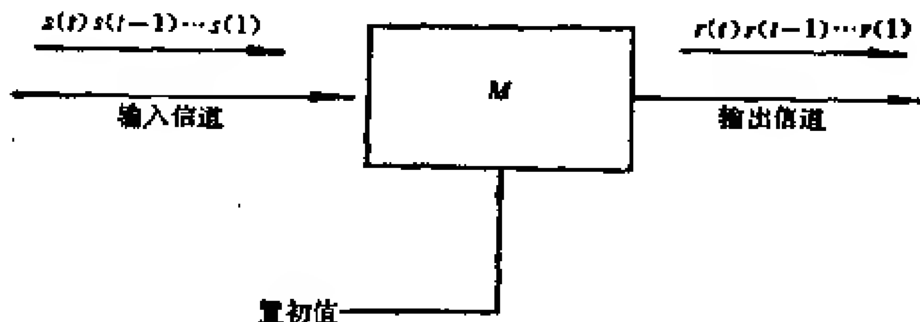


图 8-3.1

假设机器 M 在时间 $t=t_0, t_1, t_2, \cdots$ 工作，其中初始时间 t_0 及时间间隔 $\Delta t_i=t_i-t_{i-1}$ 都是任意的。为了简化起见，常把它们表示为 $t=0, 1, 2, \cdots$。在 $t=0$ 时，将已知的初始条件作为初值，在以

后每一瞬间 t，通过输入信道，机器 M 收到一个输入信号 $s(t)$，它就产生一个输出信号 $r(t)$，通过输出信道输出。提供给机器的一串输入信号 $s(1)s(2)\cdots s(t)$ 称为一个激励；所产生的输出符号串称为 M 对于此激励的响应。

所有输入符号组成的集合称为输入符号集(输入字母表)，记作 S。所有输出符号组成的集合称为输出符号集(输出字母表)，记作 R。

现实世界中的机器都可认为由有限个部件组成，且每个部件都有有限个状态。假设机器 M 由 N 个部件组成，$q^{(i)}(t)$ 表示第 i 个部件在瞬间 t 的状态，那么，在时间 t，M 的状态是一个 N 有序组

$$\langle q^{(1)}(t),\ q^{(2)}(t),\ \cdots,\ q^{(N)}(t)\rangle$$

故，M 总状态的最大可能数是所有部件状态数的积。若每一部件的状态数不超过 K，则 M 的状态数不超过 K^N。我们用 $q(t)$ 表示 M 在时间 t 的状态，即 $q(t)=\langle q^{(1)}(t),\ q^{(2)}(t),\ \cdots,\ q^{(N)}(t)\rangle$，所有不同的 $q(t)$ 组成的集合称为状态集，记作 Q。机器 M 在 $t=0$ 所处的状态称为初始状态(初态)，记作 q_I，即 $q_I=q(0)$。

机器 M 在接收到输入信号 $s(t)$ 时，它将产生一个输出 $r(t)$，同时，状态从 $q(t-1)$ 转换到 $q(t)$。$r(t)$ 和 $q(t)$ 不仅与 $s(t)$ 有关，而且与机器在前一瞬间的状态 $q(t-1)$ 有关。因此，存在一个函数 f，用它来描述机器的状态：

$$q(t)=f(q(t-1),\ s(t)) \quad t\geqslant 1$$

它称为状态转换函数。它的定义域是状态集 Q 与输入符号集 S 的笛卡尔积，值域是状态集的子集，即

$$f:\ Q\times S\rightarrow Q$$

还存在一个函数 g，用它来描述机器的输出：

$$r(t)=g(q(t-1),\ s(t)) \quad t\geqslant 1$$

它称为输出函数。它的定义域也是 $Q\times S$，值域是输出字母表 R，即

$$g:\ Q\times S\rightarrow R$$

这类机器当它处于状态 $q(t-1)$ 时且接收到输入信号 $s(t)$，状态就转向唯一确定的下一状态 $q(t)$，且产生一个确定的输出信号 $r(t)$，称这类机器是确定型的。

状态数是有限的机器称为有限状态机。它由下面四个部分组成。

1．三个有限集 S、R 和 Q。

2．状态转换函数 f。

3．输出函数 g。

4．初态 q_I。

定义 8-3.1 一台转换赋值有限状态机是一个六有序组

$$M=(Q, S, R, f, g, q_I)$$

其中：Q 是状态的有限集合

S 是有限输入字母表

R 是有限输出字母表

f 是状态转换函数

$$f: Q\times S\to Q$$

g 是输出函数

$$g: Q\times S\to R$$

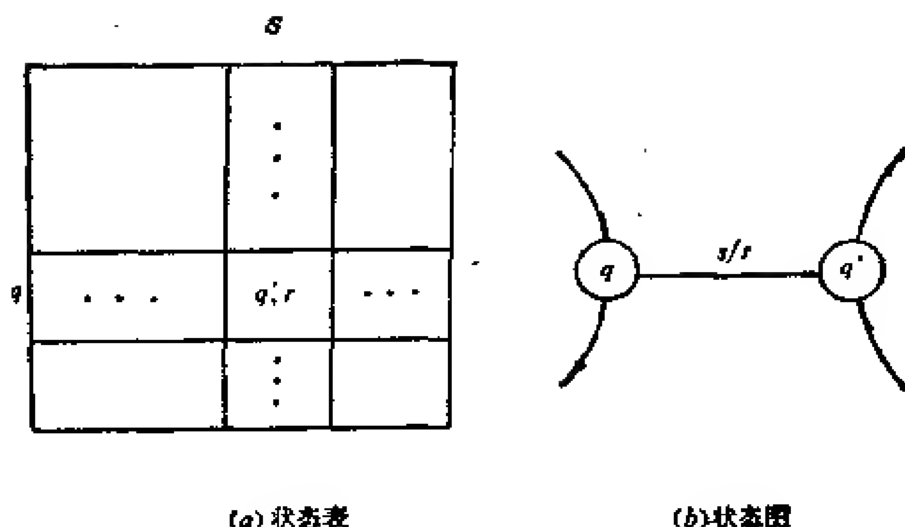
$q_I\in Q$ 是初态

这类自动机，又称米兰(Melay)机，它的输出符号不仅与机器所处的状态有关，而且与输入字母有关，即需考虑状态 $q(t)$ 是从哪一状态转换而来，因此就称为转换赋值有限状态机。

描述有限状态机有两种方法：状态表和状态图。

状态表可同时表示两个函数，表的左端从上到下标记所有状态，常把 q_I 放在最上面，表的上方从左到右标记所有输入符号，因此，表的行数是 $|Q|$，表的列数是 $|S|$。相应于状态 q 的行与相应于输入符号 s 的列的交错处，写上下一状态 $q'=f(q, s)$ 和输出符号 $r=g(q, s)$，如图 8-3.2(a)所示。

状态图是一个有向图，其中每一结点表示机器的一个状态，每一有向弧指出从一个状态到另一个状态的转换，此有向弧上加以



(a) 状态表　　　　(b)状态图

图 8–3.2

标记 s/r，其中 r，s 分别表示相应的输出符号和输入符号，对于初态 q_I，用一个指向它的箭头来标明，如图 8–3.2(b)所示。

在图 8–3.2 中都表示，$q'=f(q, s)$，$r=g(q, s)$，我们经常也将它们记为

$$q \xrightarrow{s/r} q'$$

这样，对于激励 $s(1)s(2)\cdots s(t)$ 产生响应 $r(1)r(2)\cdots r(t)$ 和状态序列 $q(0)q(1)\cdots q(t)$，可以记为

$$q(0)\xrightarrow{s(1)/r(1)}q(1)\xrightarrow{s(2)/r(2)}q(2)\rightarrow\cdots$$
$$\rightarrow q(t-1)\xrightarrow{s(t)/r(t)}q(t)$$

如果令 $\omega=s(1)s(2)\cdots s(t)$ 表示激励，$\varphi=r(1)r(2)\cdots r(t)$ 表示响应，那么，机器的动作可以用更紧凑的记号表示为

$$q\overset{\omega/\varphi}{\Rightarrow}q'\quad\begin{cases}q=q(0)\\q'=q(t)\end{cases}$$

下面考察几个例子。

例题 1 （模 3 计数器） 设计一台有限状态机 M_1，它的输出是已经输入符号数的模 3 数。

解 由于输出是输入符号数的模 3 数，而与具体的输入符号无关，所以，可以认为输入字母集是单字母集，即 $S=\{a\}$。而输出字母集 R 应包括三个元素 0，1 和 2，即 $R=\{0, 1, 2\}$。要求机器的状态能“记住”已经输入符号数

的模 3 数，所以，状态集也应有三个状态，即 $Q=\{A, B, C\}$，设 t 表示激励 ω 最末符号所对应的瞬间，状态 $q(t)$ 的解释为

$$q(t)=\begin{cases} A & 当\ |\omega| \bmod 3=0 \\ B & 当\ |\omega| \bmod 3=1 \\ C & 当\ |\omega| \bmod 3=2 \end{cases}$$

它的状态转换函数应为

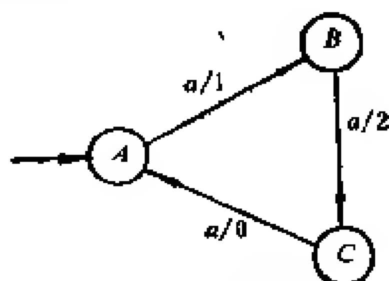
$$f(A, a)=B,\ f(B, a)=C,\ f(C, a)=A$$

它的输出函数应为

$$g(A, a)=1,\ g(B, a)=2,\ g(C, a)=0$$

因此 $$M_1=(\{A, B, C\}, \{a\}, \{0, 1, 2\}, f, g, A)$$

它的状态图和状态表如图 8-3.3 所示。



(a) 状态图

	a
A	B, 1
B	C, 2
C	A, 0

(b) 状态表

图 8-3.3

对于激励 $aaaa$，M_1 的动作是

$$A \xrightarrow{a/1} B \xrightarrow{a/2} C \xrightarrow{a/0} A \xrightarrow{a/1} B$$

所以，它的响应是 1201，状态序列是 $ABCAB$。

例题 2 （奇偶校验器） 设计一台有限状态机 M_2，它的输入是 $\{0, 1\}$ 上的符号串，要求输入串有奇数个 1 时输出 1，输入串有偶数个 1 时输出 0。

解 显然 $S=R=\{0, 1\}$。

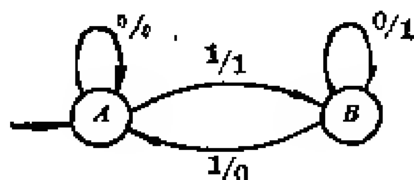
给定输入串 ω，令 $\omega=\omega_1 s$，其中 $\omega_1 \in \{0, 1\}^*$，$s \in \{0, 1\}$。如果 $s=0$，则 ω 中所含 1 个数的奇偶性与 ω_1 相同。如果 $s=1$，则 ω 中所含 1 个数的奇偶性与 ω_1 相反。由此可知，M_2 只需要两个状态，状态 A 表示已输入的串中 1 的个数为偶数，状态 B 表示已输入的串中 1 的个数为奇数。所以，$Q=\{A, B\}$。它的状态转换函数为

$$f(A, 0)=A,\ f(A, 1)=B$$
$$f(B, 0)=B,\ f(B, 1)=A$$

它的输出函数为

$$g(A, 0)=0,\quad g(A, 1)=1$$
$$g(B, 0)=1,\quad g(B, 1)=0$$

因此 $$M_2=(\{A,\ B\},\ \{0,\ 1\},\ \{0,\ 1\},\ f,\ g,\ A)$$
它的状态图和状态表如图 8-3.4 所示。



(a) 状态图

	0	1
A	A, 0	B, 1
B	B, 1	A, 0

(b) 状态表

图 8-3.4

对于激励 010011, M_2 的动作是

$$A\xrightarrow{0/0}A\xrightarrow{1/1}B\xrightarrow{0/1}B\xrightarrow{0/1}B\xrightarrow{1/0}A\xrightarrow{1/1}B$$

因此,响应是 011101, 状态序列是 $AABBBAB$。

例题 8 (二单位延迟器) 设计一台有限状态机 M_3, 它的输入字母表是 $\{0,\ 1\}$, 要求输出串是输入串延迟两个时间单位的重复,即

$$r(t)=s(t-2)\quad t\geqslant 3$$

解 显然 $S=R=\{0,\ 1\}$。按照题意, $r(t)$ 只有当 $t\geqslant 3$ 时才由输入决定, 不妨规定 $r(1)=r(2)=0$。由于 M_3 的状态依赖于最后两个输入符 $s(t-2)s(t-1)$, 所以,它应有 $2^2=4$ 个状态, 故可规定

$s(t-2)$	$s(t-1)$	M_3 的状态
0	0	A
1	0	B
1	1	C
0	1	D

所以 $$Q=\{A,\ B,\ C,\ D\}$$

它的状态转换函数是

$$f(A,\ 0)=A,\ f(B,\ 0)=A,\ f(C,\ 0)=B,\ f(D,\ 0)=B$$

$$f(A,\ 1)=D,\ f(B,\ 1)=D,\ f(C,\ 1)=C,\ f(D,\ 1)=C$$

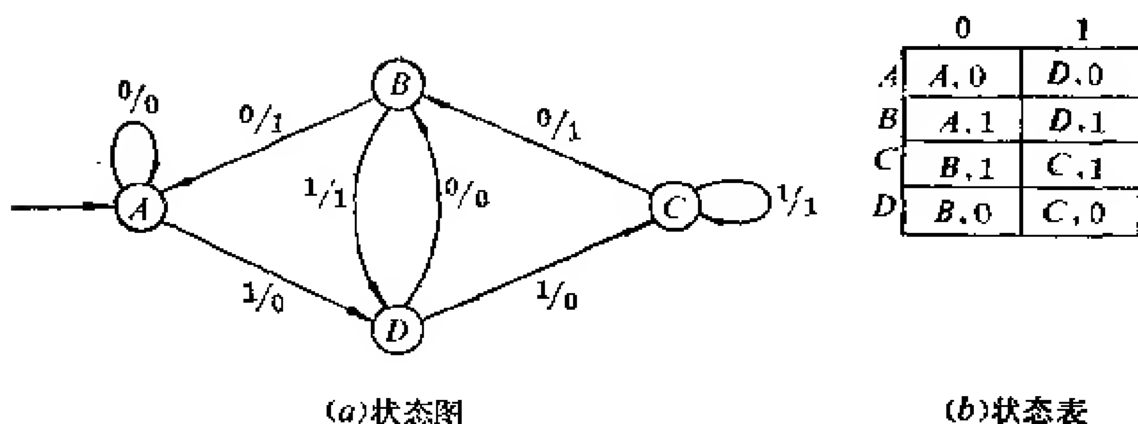
它的输出函数是

$$g(A,\ 0)=0,\ g(B,\ 0)=1,\ g(C,\ 0)=1,\ g(D,\ 0)=0$$

$$g(A,\ 1)=0,\ g(B,\ 1)=1,\ g(C,\ 1)=1,\ g(D,\ 1)=0$$

因此 $$M_3=(\{A,\ B,\ C,\ D\},\ \{0,\ 1\},\ \{0,\ 1\},\ f,\ g,\ A)$$

它的状态图和状态表如图 8-3.5 所示。



	0	1
A	A, 0	D, 0
B	A, 1	D, 1
C	B, 1	C, 1
D	B, 0	C, 0

(a)状态图　　　　　(b)状态表

图　8-3.5

对于激励 000110100, M_3 的动作是

$$A \xrightarrow{0/0} A \xrightarrow{0/0} A \xrightarrow{0/0} A \xrightarrow{1/0} D \xrightarrow{1/0} C$$

$$\xrightarrow{0/1} B \xrightarrow{1/1} D \xrightarrow{0/0} B \xrightarrow{0/1} A$$

因此,响应是 000001101, 状态序列是 $AAAADCBDBA$。

还有一类有限状态机,其输出只与到达状态有关,而与从哪个状态转换来的无关。如例题 2 的奇偶校验器,只要转向状态 A, 输出就是 0, 只要转向状态 B, 输出就是 1。象这类有限状态机,称为状态赋值机,又称摩尔(Moore)机。

定义 8-3.2　一台状态赋值有限状态机是六有序组

$$M=(Q,\ S,\ R,\ f,\ h,\ q_I)$$

其中: Q 是状态的有限集合

S 是有限输入字母表

R 是有限输出字母表

f 是状态转换函数

$$f:\ Q\times S\rightarrow Q$$

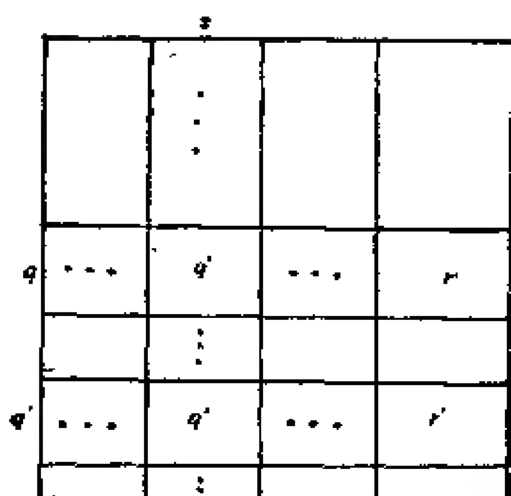
h 是输出函数

$$h:\ Q\rightarrow R$$

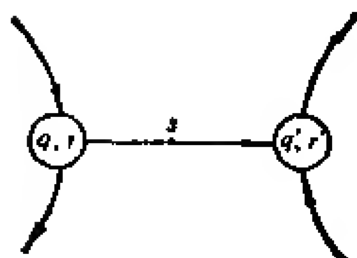
$q_I\in Q$ 是初态

状态赋值机的状态表和状态图如图 8-3.6 所示。

状态表中, 相应于状态 q 的行与相应于输入字母 s 的列的交错处, 写上下一状态 $q'=f(q,\ s)$, 表的最右一列写上各状态的对



(a)状态表



(b)状态图

图 8-3.6

应输出。状态图中，每一结点，用一个状态和它相应的输出来标识，每一有向弧指出从一个状态到另一状态的转换，此有向弧上，加以标记如 s 作为相应的输入符号。图 8-3.6(a) 和 (b) 都表示 $q'=f(q, s)$, $h(q)=r$, $h(q')=r'$。用状态序列也可表示为

$$\langle q, r\rangle \xrightarrow{s} \langle q', r'\rangle$$

例题 4 （模 4 往返计数器） 设计一台有限状态机 M_4，它的输入字母表 $S=\{0, 1\}$，要求输出

$$r(t)=[N_1(\omega)-N_0(\omega)] \bmod 4$$

其中 $\omega=s(1)s(2)\cdots s(t)$ 是输入串，$N_0(\omega)$ 是 ω 中 0 的个数，$N_1(\omega)$ 是 ω 中 1 的个数。

解 根据输出的要求，有 $R=\{0, 1, 2, 3\}$。M_4 应有四个状态，状态 A 表示 $r(t)=0$，B 表示 $r(t)=1$，C 表示 $r(t)=2$，D 表示 $r(t)=3$。这是一台状态赋值机。它的状态转换函数为

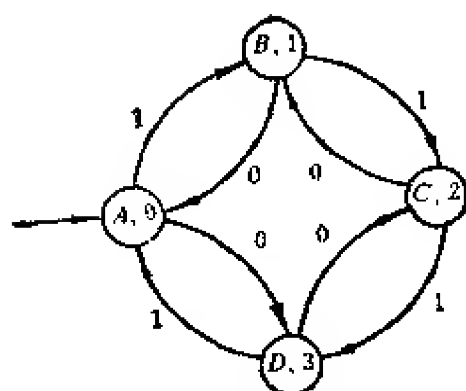
$$f(A, 0)=D,\ f(B, 0)=A,\ f(C, 0)=B,\ f(D, 0)=C$$
$$f(A, 1)=B,\ f(B, 1)=C,\ f(C, 1)=D,\ f(D, 1)=A$$

它的输出函数是

$$h(A)=0,\ h(B)=1,\ h(C)=2,\ h(D)=3$$

因此 $$M_4=(\{A, B, C, D\}, \{0, 1\}, \{0, 1, 2, 3\}, f, h, A)$$

它的状态图和状态表如图 8-3.7 所示。



(a)状态图

	0	1	
A	D	B	0
B	A	C	1
C	B	D	2
D	C	A	3

(b)状态表

图 8-3.7

例题 5 （语言识别器） 设计一台有限状态机 M_5，它接受一个二进制串，当且仅当此串由 1 开始，且其中恰含一个 0，这种串可表示为 11^*01^*。

解 我们可用输出 0，1 表示输入串 ω 是否被 M_5 接受，如果输入串 ω 使 M_5 从初态最后转向一个状态，它的输出是 1，则表示 ω 被 M_5 接受；它的输出是 0，则表示 ω 被 M_5 拒绝。

下面考察 M_5 至少需要多少个状态。

(1) 初态 A，输出 0：

M_5 从状态 A 出发。

(2) 陷阱状态 B，输出 0：

如果输入串的第一个字母是 0，此串必被 M_5 拒绝，此时 M_5 进入状态 B，M_5 一旦进入状态 B，无论输入什么字母，不再能转向其他状态。

(3) 可能接受状态 C，输出 0：

如果输入串的第一个字母是 1，M_5 进入状态 C，表示此输入串可能被接受。

(a) 继续输入 1，则 M_5 仍处于状态 C。

(b) 继续输入 0，则 M_5 进入状态 D。

(4) 接受状态 D，输出 1：

M_5 进入状态 D，表示此输入串被 M_5 接受，输出 1。

(a) 继续输入 1，M_5 仍处于状态 D。

(b) 继续输入 0，此输入串中已经有两个 0，这种串必被 M_5 拒绝，故 M_5 再次进入陷阱状态 B。所以，

$$M_5=(\{A, B, C, D\}, \{0, 1\}, \{0, 1\}, f, h, A)$$

其中状态转换函数 f 是

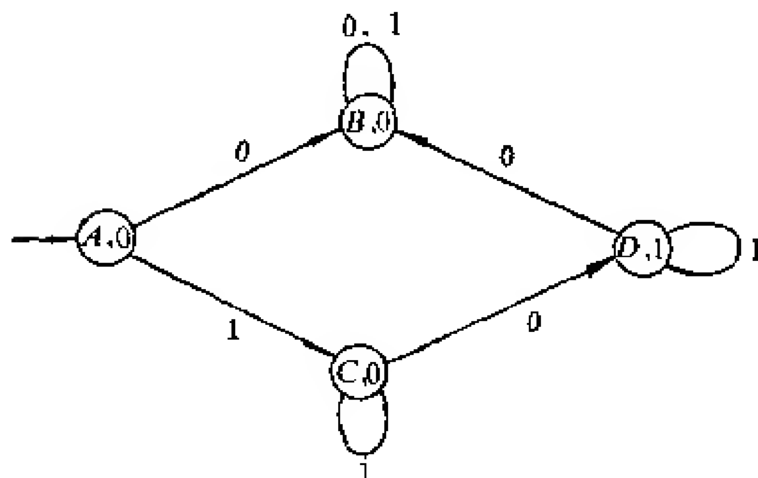
$$f(A, 0)=B, f(B, 0)=B, f(C, 0)=D, f(D, 0)=B,$$

$$f(A,1)=C,\ f(B,1)=B,\ f(C,1)=C,\ f(D,1)=D$$

它的输出函数 h 是

$$h(A)=0,\ h(B)=0,\ h(C)=0,\ h(D)=1$$

它的状态图和状态表如图 8-3.8 所示。



(a)状态图

	0	1	
A	B	C	0
B	B	B	0
C	D	C	0
D	B	D	1

(b)状态表

图 8-3.8

8-3 习题

(1) 构造有限状态机 $M=(Q,S,R,f,g,q_1)$,其中 $S=R=\{0,1,2,3\}$, 对于 $t>2$, 有 $r(t)=m(t)+n(t)$, 这里

$$m(t)=\begin{cases}2 & \text{如果 } s(t-1) \text{ 是 0 或 2} \\ 0 & \text{其它}\end{cases}$$

$$n(t)=\begin{cases}1 & \text{如果 } s(t-2) \text{ 是 1 或 3} \\ 0 & \text{其它}\end{cases}$$

如果 $s(-1)=s(0)=0$, 确定 $r(1)$ 和 $r(2)$。

(2) 设 $S=\{a,b,c\}$, 对于 S 中每一符号 s 和 S^* 中每一串 ω, 定义: $N_s(\omega)=\omega$ 中 s 出现的次数。给出转换赋值机 $M=(Q,S,R,f,g,q_1)$的状态图,对于输入串 ω, 它的最终输出是

$$r=(N_a(\omega)+2N_b(\omega)-3N_c(\omega))\bmod 5$$

求激励是 $abbccbaabc$ 的响应。

(3) 已知有限状态机的状态图,写出相应的状态表。

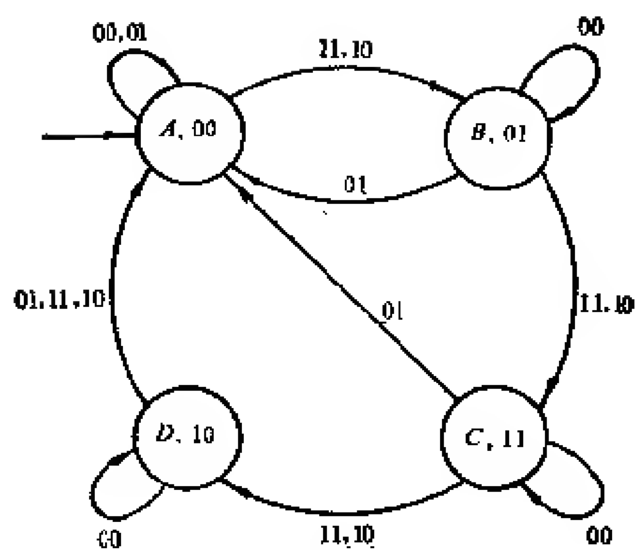


图 8-3.9

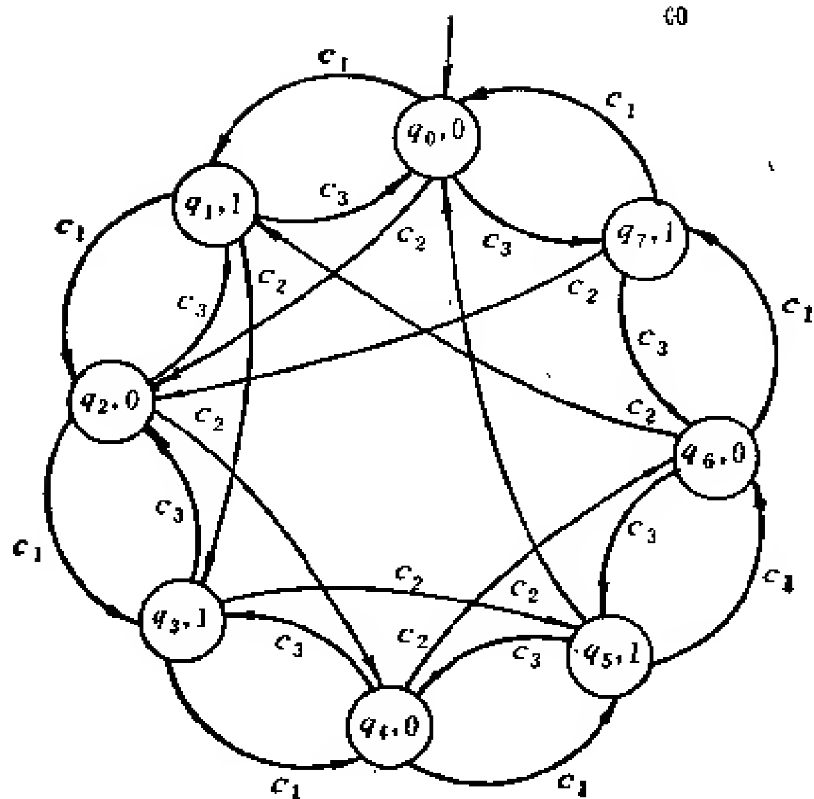


图 8-3.10

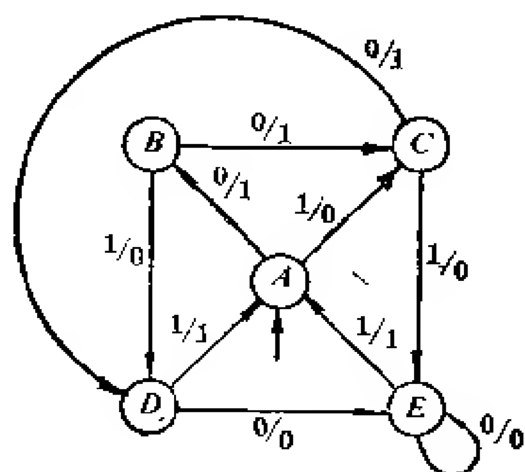


图 8-3.11

(4) 给定有限状态机的状态表，画出相应的状态图。

a)

	0	1	
A	C	B	0
B	C	D	0
C	D	B	0
D	B	A	1

b)

	0	1
q_0	q_0, 0	q_1, 0
q_1	q_0, 0	q_2, 0
q_2	q_0, 0	q_2, 1

(5) 设 M 是 n 个状态的有限状态机，如果有一个激励，将 M 从状态 q_I 转向状态 q，证明必存在一个长度小于 n 的激励，使 M 从状态 q_I 转向状态 q。

(6) 设计一台有限状态机 M，其中 $S=B=\{0, 1\}$，当输入串中有三个连续的 0 或 1 时，它输出 1，其它均输出 0。

(7) 设计一台有限状态机，其中 $S=\{a, b\}$，当且仅当输入符号串中包含两个连续的 a 或两个连续的 b 时，输出为 1，否则为 0。

*(8) 给定有限状态机 M_1 和 M_2 的状态图。

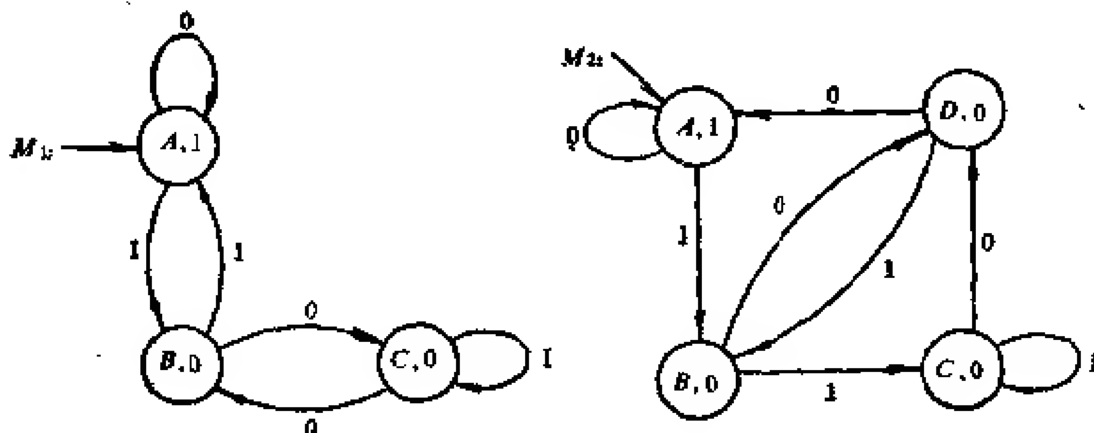


图 8-3.12

证明

a) 当且仅当输入串是能被 3 整除的二进制数时，有限状态机 M_1 输出为 1，其它为 0。

b) 当且仅当输入串是能被 4 整除的二进制数时，有限状态机 M_2 输出为 1，其它为 0。

8-4　两类自动机的转换

在 8-3 节例题 2 提到的奇偶校验器是一台转换赋值机，但它有这样一个特点，只要转换到状态 A，输出就是 0，只要转换到状态 B，输出就是 1，它与图 8-4.1 所示的状态赋值机 M_2' 的功能相同。

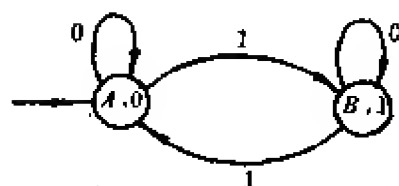


图　8-4.1

下面讨论两类自动机的转换问题。

定义 8-4.1　设 M 是有限状态机，状态函数

$$f:\ Q\times S\rightarrow Q$$

如果 $f(q,\ s)=q'$，称 q' 是状态 q 的 s——后继，记为

$$q\xrightarrow{s}q'^{\text{〔注〕}}$$

如果输入串 $\omega=s(1)s(2)\cdots s(t)$ 将 M 从状态 $q=q(0)$ 转向 $q'=q(t)$，即

$$q=q(0)\xrightarrow{s(1)}q(1)\xrightarrow{s(2)}q(2)\xrightarrow{s(3)}\cdots\xrightarrow{s(t)}q(t)=q'$$

称状态 q' 是状态 q 的 ω-后继，记为

$$q\overset{\omega}{\Rightarrow}q'$$

并称 $q(0)q(1)q(2)\cdots q(t)$ 是 ω 的可接受状态序列。

在上节例题 2 中，状态 B 是状态 A 的 00100-后继，状态 B 也是状态 A 的 010011-后继，可以分别记为

$$A\overset{00100}{\Rightarrow}B,\qquad A\overset{010011}{\Rightarrow}B$$

00100 的可接受状态序列是 $AAABBB$，010011 的可接受状态序列是 $AABBBAB$。

下面考察两类自动机对应于激励 $\omega=s(1)s(2)\cdots s(t)$ 的可接受状态序列 $q_Iq(1)q(2)\cdots q(t)$ 和响应 $r(1)r(2)\cdots r(t)$。

〔注〕　这里 $q\xrightarrow{s}q'$ 表示状态之间的转换，并不是映射记号。

(A) 可接受状态序列

$$q(1)=f(q_I,\ s(1))=f_1(q_I,\ s(1))$$

$$q(2)=f(q(1),\ s(2))=f(f_1(q_I,\ s(1)),\ s(2))$$
$$=f_2(q_I,\ s(1)s(2))=f(q_I,\ s(1)s(2))$$

$$q(3)=f(q(2),\ s(3))=f(f_2(q_I,\ s(1)s(2)),\ s(3))$$
$$=f_3(q_I,\ s(1)s(2)s(3))=f(q_I,\ s(1)s(2)s(3))$$

......

$$q(t)=f(q(t-1),\ s(t))$$
$$=f(f_{t-1}(q_I,\ s(1)s(2)\cdots s(t-1)),\ s(t))$$
$$=f_t(q_I,\ s(1)s(2)\cdots s(t))$$
$$=f(q_I,\ s(1)s(2)\cdots s(t))$$

在上述各式的最后一步删去了 f 的下标，不会引起误解，这样，我们将状态函数 f: $Q\times S\rightarrow Q$ 推广为 f: $Q\times S^+\rightarrow Q$，且有 $f(q,\ \omega a)=f(f(q,\ \omega),\ a)$，其中 $\omega\in S^+$，$a\in S$。

(B) 响应

(1) 对于转换赋值机

$$r(1)=g(q_I,\ s(1))=g_1(q_I,\ s(1))$$

$$r(2)=g(q(1),\ s(2))=g(f(q_I,\ s(1)),\ s(2))$$
$$=g_2(q_I,\ s(1)s(2))=g(q_I,\ s(1)s(2))$$

$$r(3)=g(q(2),\ s(3))=g(f(q_I,\ s(1)s(2)),\ s(3))$$
$$=g_3(q_I,\ s(1)s(2)s(3))=g(q_I,\ s(1)s(2)s(3))$$

......

$$r(t)=g(q(t-1),\ s(t))$$
$$=g(f(q_I,\ s(1)s(2)\cdots s(t-1)),\ s(t))$$
$$=g_t(q_I,\ s(1)s(2)\cdots s(t))=g(q_I,\ s(1)s(2)\cdots s(t))$$

(2) 对于状态赋值机，我们有

$$r(0)=h(q_I)$$

$$r(1)=h(q(1))=h(f(q_I,\ s(1)))=h_1(q_I,\ s(1))$$
$$=h(q_I,\ s(1))$$

$$r(2)=h(q(2))=h(f(q_I,\ s(1)s(2)))$$
$$=h_2(q_I,\ s(1)s(2))=h(q_I,\ s(1)s(2))$$
$$r(3)=h(q(3))=h(f(q_I,\ s(1)s(2)s(3)))$$
$$=h_3(q_I,\ s(1)s(2)s(3))=h(q_I,\ s(1)s(2)s(3))$$
$$\cdots\cdots$$
$$r(t)=h(q(t))=h(f(q_I,\ s(1)s(2)\cdots s(t)))$$
$$=h_t(q_I,\ s(1)s(2)\cdots s(t))=h(q_I,\ s(1)s(2)\cdots s(t))$$

因此,对于两类自动机,它的输出可统一记为

$$r(t)=O(q_I,\ s(1)s(2)\cdots s(t))\quad (t\geqslant 1)$$

我们约定,以后讨论的结果如果对两类自动机都适用时,输出函数就用O来表示。这样,输出函数就推广为$O: Q\times S^+\rightarrow R$,且有$O(q_I,\ \omega a)=O(f(q_I,\ \omega),\ a)$,其中$\omega\in S^+$,$a\in S$。

由于状态赋值机有$r(0)=h(q_I)$的存在,所以,转换赋值机与状态赋值机有一个本质的区别:对于空串,前者无响应,后者有一个确定的响应$h(q_I)$。

定理8-4.1 对于有限状态机M,我们有

$$f(q,\ \omega\varphi)=f(f(q,\ \omega),\ \varphi)$$
$$O(q,\ \omega\varphi)=O(f(q,\ \omega),\ \varphi)$$

其中,q是q_I的ψ-后继,ω,$\varphi\in S^+$,$\psi\in S^*$。

证明 先证 $f(q_I,\ \omega\varphi)=f(f(q_I,\ \omega),\ \varphi)$

对$|\varphi|$进行归纳证明

当$|\varphi|=1$时,φ是一个输入字母a,故有

$$f(q_I,\ \omega a)=f(f(q_I,\ \omega),\ a)$$

设$|\varphi|=k$时,上式成立。

当$|\varphi|=k+1$时,此时,令$\varphi=\varphi' a$,其中$|\varphi'|=k$:

$$f(q_I,\ \omega\varphi)=f(q_I,\ \omega\varphi' a)=f(f(q_I,\ \omega\varphi'),\ a)$$
$$=f(f(f(q_I,\ \omega),\ \varphi'),\ a)=f(f(q',\ \varphi'),\ a)$$
$$=f(q',\ \varphi' a)=f(q',\ \varphi)=f(f(q_I,\ \omega),\ \varphi)$$

所以,我们有 $f(q_I,\ \omega\varphi)=f(f(q_I,\ \omega),\ \varphi)$

设q是q_I的ψ-后继,即$q=f(q_I,\ \psi)$,此时

$$f(q,\ \omega\varphi)=f(f(q_I,\ \psi),\ \omega\varphi)=f(q_I,\ \psi\omega\varphi)$$
$$=f(f(q_I,\ \psi\omega),\ \varphi)=f(f(f(q_I,\ \psi),\ \omega),\ \varphi)$$
$$=f(f(q,\ \omega),\ \varphi)$$

因此，我们有 $f(q,\ \omega\varphi)=f(f(q,\ \omega),\ \varphi)$

对于输出函数可以类似证明，留作习题。 □

定理 8-4.1 具有下列实际意义，$f(q,\ \omega\varphi)$ 是自动机 M 处于状态 q，输入字符串 $\omega\varphi$ 后的状态，而 $f(f(q,\ \omega),\ \varphi)$ 是自动机 M 处于状态 q，先输入字符串 ω，它处于状态 $f(q,\ \omega)$，然后再输入字符串 φ 后的状态，它们应该是一样的。对于输出函数也有类似的解释。

例如 8-3 节中奇偶校验器 M_2，输入 00100，M_2 处于状态 B，如果先输入 001，M_2 处于状态 B，再输入 00，M_2 仍处于状态 B。

定义 8-4.2 给定状态赋值机 M_s 和转换赋值机 M_t，如果对每一激励，M_s 的响应恰等于 M_t 的响应前面加一任意且确定的输出符号，称 M_s 和 M_t 是相似的。

图 8-4.2 给出定义 8-4.2 的图解。对自动机 M_t 和 M_s 提供相同的激励 ω，那么，M_t 的响应是 φ，M_s 的响应是 $r_0\varphi$，这里 r_0 是一固定的输出字母，与激励 ω 无关。事实上 r_0 就是状态赋值机 M_s 对于空串 λ 的响应，即对应初态 q_I 的输出。

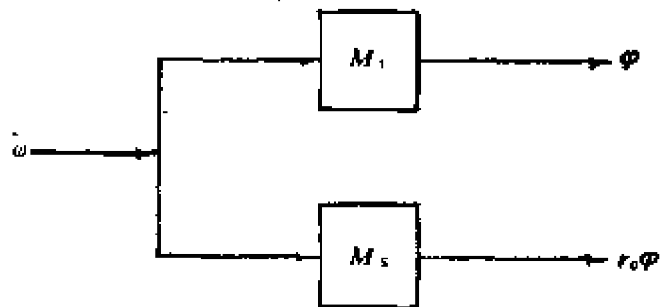


图 8-4.2

例如，图 8-4.1 的状态赋值机与图 8-3.4 的转换赋值机是相似的。

定理 8-4.2 对于每一台状态赋值机 M_s，存在一台相似的转换赋值机 M_t。反之，对于每一台转换赋值机 M_t，也存在一台相似的状态赋值机 M_s。

证明

(A) 从 M_s 构造相似的 M_t。

我们将 M_s 的状态集 Q, 输入字母表 S, 输出字母表 R, 初始状态 q_I 和状态转换函数 f 分别作为 M_t 的状态集 Q, 输入字母表 S, 输出字母表 R, 初始状态 q_I 和状态转换函数 f。定义 M_t 的输出函数 g: 当 M_s 中状态 q 有输出 r 时,那么,在 M_t 中所有转向 q 的转换就赋值输出 r。具体构造如下:

如果 $$M_s=(Q, S, R, f, h, q_I)$$

那么 $$M_t=(Q, S, R, f, g, q_I)$$

其中 $$g(q, s)=h(f(q, s)),\quad q\in Q,\ s\in S$$

显然,对于激励 ω, M_t 的响应是 M_s 的响应中除去第一个字母所剩下的输出字符串,因此, M_t 相似于 M_s。

(B) 从 M_t 构造相似的 M_s。

它比较复杂,我们不能简单地将上面的构造过程逆转。因为 M_t 中可能有一个状态 q, 对于 q 来说,存在多个输入转换,它们标以不同的输出符号。例如图 8-3.5 中状态 A, 如果它是从 A 自身转换来,输出就是 0, 从 R 转换来,输出就是 1。为了克服此困难,我们将 M_t 中的状态和输出符号组成的序偶,作为 M_s 的状态。我们规定若 M_t 进入状态 q 且产生输出符号 r, 那么, M_s 就进入状态 $\langle q, r\rangle$。对于状态 $\langle q, r\rangle$, 它的输出是 r。具体构造如下:

如果 $$M_t=(Q_t, S, R, f_t, g, q_I)$$

那么 $$M_s=(Q_s, S, R, f_s, h, \langle q_I, r_0\rangle)$$

其中 $$Q_s=Q_t\times R$$

函数 f_s, h 定义如下:当 M_t 有 $q\xrightarrow{s/r}q'$ 那么, M_s 有

$$\langle\langle q, r'\rangle, r'\rangle\xrightarrow{s}\langle\langle q', r\rangle, r\rangle$$

其中 $r'\in R$, r' 取遍 R 中所有字母。即

$$f_s(\langle q, r'\rangle, s)=\langle q', r\rangle\quad r'\in R$$

$$h(\langle q', r\rangle)=r$$

对于所有 $\langle q_I, r\rangle$ 中可任取一个 $\langle q_I, r_0\rangle$ 作为 M_s 的初态。显然,对于激励 ω, 当 M_t 的响应是 φ 时, M_s 的响应必是 $r_0\varphi$, 因此, M_s 相似于 M_t。 □

显然，与图 8-3.7所示的模 4 往返计数器 M_4 相似的转换赋值机 M_4' 如图 8-4.3 所示。

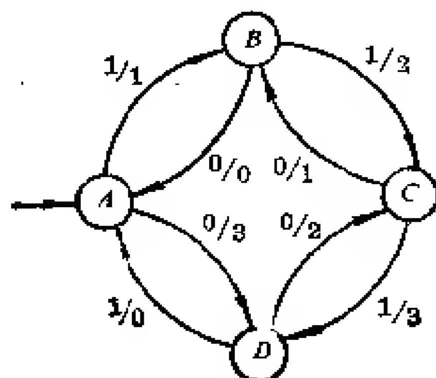


图 8-4.3

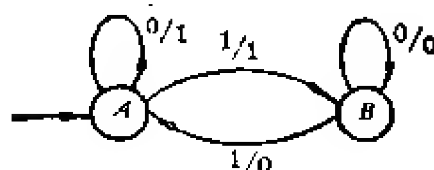


图 8-4.4

例题 1 给定 $M_t=(\{A, B\}, \{0, 1\}, \{0, 1\}, f_t, g, A)$，构造一台与它相似的 M_s。M_t 的状态图如图 8-4.4 所示。

解 $M_s=(Q_s, \{0, 1\}, \{0, 1\}, f_s, h, \langle A, r_0\rangle)$

其中 $Q_s=Q_t\times R=\{\langle A, 0\rangle, \langle A, 1\rangle, \langle B, 0\rangle, \langle B, 1\rangle\}$

表 8-4.1 给出由 M_t 的转换所构造的相应的 M_s 中的转换。

表 8-4.1

	M_t	M_s
1	$A\xrightarrow{0/1}A$	$\langle\langle A, 0\rangle, 0\rangle\xrightarrow{0}\langle\langle A, 1\rangle, 1\rangle$ $\langle\langle A, 1\rangle, 1\rangle\xrightarrow{0}\langle\langle A, 1\rangle, 1\rangle$
2	$A\xrightarrow{1/1}B$	$\langle\langle A, 0\rangle, 0\rangle\xrightarrow{1}\langle\langle B, 1\rangle, 1\rangle$ $\langle\langle A, 1\rangle, 1\rangle\xrightarrow{1}\langle\langle B, 1\rangle, 1\rangle$
3	$B\xrightarrow{0/0}B$	$\langle\langle B, 0\rangle, 0\rangle\xrightarrow{0}\langle\langle B, 0\rangle, 0\rangle$ $\langle\langle B, 1\rangle, 1\rangle\xrightarrow{0}\langle\langle B, 0\rangle, 0\rangle$
4	$B\xrightarrow{1/0}A$	$\langle\langle B, 0\rangle, 0\rangle\xrightarrow{1}\langle\langle A, 0\rangle, 0\rangle$ $\langle\langle B, 1\rangle, 1\rangle\xrightarrow{1}\langle\langle A, 0\rangle, 0\rangle$

因此，M_s 的状态函数 f_s 定义为

$$f_s(\langle A, 0\rangle, 0)=\langle A, 1\rangle$$

$$f_s(\langle A, 0\rangle, 1)=\langle B, 1\rangle$$

$f_s(\langle A, 1\rangle, 0) = \langle A, 1\rangle$

$f_s(\langle A, 1\rangle, 1) = \langle B, 1\rangle$

$f_s(\langle B, 0\rangle, 0) = \langle B, 0\rangle$

$f_s(\langle B, 0\rangle, 1) = \langle A, 0\rangle$

$f_s(\langle B, 1\rangle, 0) = \langle B, 0\rangle$

$f_s(\langle B, 1\rangle, 1) = \langle A, 0\rangle$

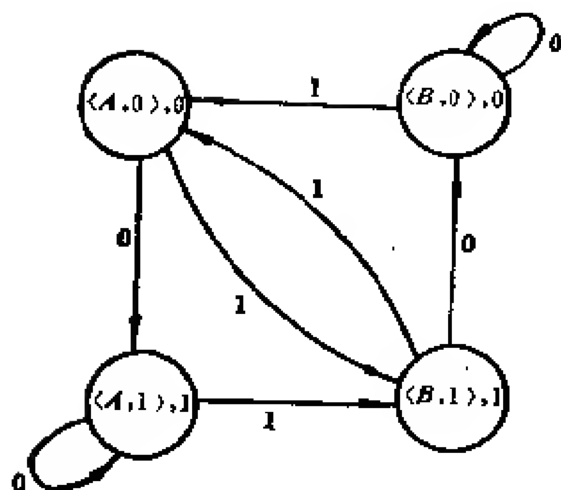


图 8-4.5

M_s 的输出函数 h 定义为

$h(\langle A, 0\rangle) = 0$

$h(\langle A, 1\rangle) = 1$

$h(\langle B, 0\rangle) = 0$

$h(\langle B, 1\rangle) = 1$

M_s 的状态图如图 8-4.5 所示。

状态 $\langle A, 0\rangle$ 和 $\langle A, 1\rangle$ 都可作为 M_s 的初态。

对于激励 101101，M_t 的响应是 100100。在 M_s 中，如果以 $\langle A, 0\rangle$ 作为初态，响应是 0100100。如果以 $\langle A, 1\rangle$ 作为初态，响应是 1100100。

8-4 习题

(1) 给定有限状态机 $M = (Q, S, R, f, h, A)$，它的状态图如图 8-4.6 所示。

a) 求状态 A 的 01110 的后继以及可接受状态序列。

b) 求状态 E 的 100101 的后继以及可接受状态序列。

c) 验证

$f(f(A, 010), 110) = f(A, 010110)$

$h(f(A, 010), 110) = h(A, 010110)$

d) 求 M 对于激励 010110 的响应。

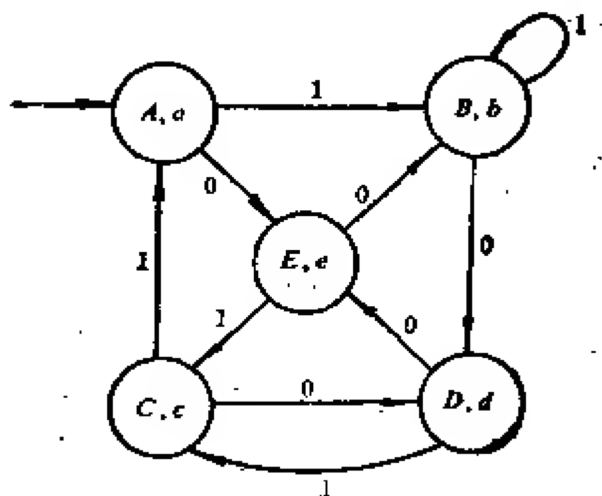


图 8-4.6

e) 构造一台与 M 相似的转换赋值机，并求它对于激励 010110 的响应。

(2) 完成定理 8-4.1 的证明。

(3) 给定有限状态机 $M=(Q, S, R, f, g, q_1)$，它的状态图如图 8-4.7 所示。

a) 求状态 q_2 的 $aabba$ 的后继以及可接受状态序列。

b) 求状态 q_3 的 $bbaaba$ 的后继以及可接受状态序列。

c) 验证

$f(f(q_2, aba), aba)=f(q_2, abaaba)$

$g(f(q_2, aba), aba)=g(q_2, abaaba)$

d) 求 M 对于激励 $abaaba$ 的响应。

e) 构造一台与 M 相似的状态赋值机，并求它对于激励 $abaaba$ 的响应。

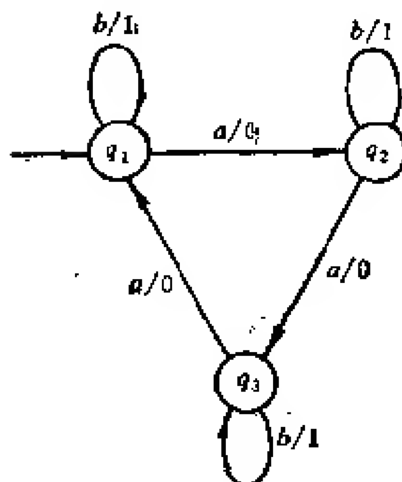


图 8-4.7

(4) 构造一台与图 8-4.5 相似的转换赋值机。

(5) 设 M_s 是与给定的转换赋值机 M_t 相似的状态赋值机，对于同一激励，M_s 的响应比 M_t 的响应多一个首字母，请对 M_t 稍作修改，使它们的响应相同。

8-5 有限状态机的简化

从上节中知道，给定一台转换赋值机

$$M_t=(Q, S, R, f, g, q_I)$$

它的状态数是 $|Q|$，设 M_s 是与 M_t 相似的状态赋值机，那么，M_s 的状态数是 $|Q|\times|R|$，若再构造一台与 M_s 相似的转换赋值机 $M_{t'}$，那么，$M_{t'}$ 的状态数将与 M_s 的状态数一样，为 $|Q|\times|R|$。显然，对于任一激励，M_t 与 $M_{t'}$ 的响应是一样的，即它们的功能相同。这样继续下去，可得一串状态数不断递增的转换赋值机，它们具有相同的功能。

给定一台自动机，是否可以构造出一台功能相同但状态数最少的自动机呢？这个问题对于有限状态机可予以解决。

定义 8-5.1 两台有限状态机 $M_1=(Q_1, S_1, R_1, f_1, O_1, q_I')$ 和 $M_2=(Q_2, S_2, R_2, f_2, O_2, q_I'')$，如果满足

1. $S_1=S_2$, $R_1=R_2$。

2. 对于任一非空激励ω，有$O_1(q_I', \omega)=O_2(q_I'', \omega)$。称$M_1$与$M_2$是等价的，记作$M_1 \sim M_2$。

可以验证有限状态机之间的关系$\sim$是有限状态机集合上的等价关系。

定义 8-5.2 有限状态机$M=(Q, S, R, f, O, q_I)$的两个状态q_a和q_b称为是等价的，当且仅当

$$M_a=(Q, S, R, f, O, q_a)$$

和

$$M_b=(Q, S, R, f, O, q_b)$$

是等价的，记为$q_a \sim q_b$。

同理，可以验证，状态之间的关系$\sim$是状态集合上的等价关系。

例如图 8-4.5 的状态赋值机M_s中，状态$\langle A, 0\rangle \sim \langle A, 1\rangle$，$\langle B, 0\rangle \sim \langle B, 1\rangle$。

当M是转换赋值机时，$q_a \sim q_b$表示对于任意激励ω，它们的响应是相同的。

当M是状态赋值机时，$q_a \sim q_b$表示对于任意激励ω，它们的响应中除去第一个字母外，应该是相同的。

定理 8-5.1 给定有限状态机$M=(Q, S, R, f, O, q_I)$，如果两个状态$q_a \sim q_b$，那么，对于任意激励ω，有

$$f(q_a, \omega) \sim f(q_b, \omega)$$

即等价状态的ω-后继也是等价的。

证明 因为$q_a \sim q_b$，对于任意的$\omega\varphi \in S^*$，有

$$O(q_a, \omega\varphi)=O(q_b, \omega\varphi)$$

由定理 8-4.1 可知

$$O(q_a, \omega\varphi)=O(f(q_a, \omega), \varphi)$$

$$O(q_b, \omega\varphi)=O(f(q_b, \omega), \varphi)$$

所以

$$O(f(q_a, \omega), \varphi)=O(f(q_b, \omega), \varphi)$$

因此

$$f(q_a, \omega) \sim f(q_b, \omega)$$ □

虽然输入字母表S是有限集，但输入字符串集合是无限集，因此，由定义出发判别两个状态是否等价是不可行的。为了解决

这个问题，先讨论状态之间一个较弱的关系——k 等价。

定义 8-5.3 给定有限状态机 $M=(Q, S, R, f, O, q_I)$，如果对于任意激励 ω，当 $|\omega|\leqslant k$ 时，有

$$O(q_a, \omega)=O(q_b, \omega)$$

称状态 q_a 与 q_b 是 k 等价的，记作 $q_a \overset{k}{\sim} q_b$。

显然，$\overset{k}{\sim}$ 也是状态集 Q 上一个等价关系。

我们已经知道，集合上的一个等价关系诱导该集合的一个划分。对于状态集 Q 上的 k 等价关系 $\overset{k}{\sim}$，诱导出划分 P_k

$$P_k=\{[q]_k \mid q\in Q\}$$

其中 $[q]_k=\{q' \mid q'\in Q, q' \overset{k}{\sim} q\}$。$Q$ 上的等价关系 $\sim$，诱导出划分 P

$$P=\{[q] \mid q\in Q\}$$

其中 $[q]=\{q' \mid q'\in Q, q'\sim q\}$。

由定义 8-5.2 和定义 8-5.3 可知，当 $q_a\sim q_b$ 时，必有 $q_a \overset{k}{\sim} q_b$，其中 k 为任意正整数。当 $q_a \overset{k+1}{\sim} q_b$ 时，必有 $q_a \overset{k}{\sim} q_b$。因此，划分 P_{k+1} 是划分 P_k 的加细，划分 P 是所有划分 P_k 的加细。

定理 8-5.2 如果对于某一正整数 k，$P_k=P_{k+1}$ 当且仅当 $P_k=P$。

证明 a) 用反证法

若 $P_k=P$，而 $P_{k+1}\neq P_k$，则 P_{k+1} 必是 P_k 的真加细，又因 P 是 P_{k+1} 的加细，所以，P 是 P_k 的真加细，与题设矛盾，因此 $P_{k+1}=P_k$。

b) 也用反证法

设 $P_k=P_{k+1}$ 而 $P_k\neq P$，则必有 $q_a, q_b\in Q$，$q_a \overset{k}{\sim} q_b$ 而 $q_a \not\sim q_b$。令 j 是使 q_a 与 q_b 不是 j 等价的最小正整数，显然 $j>k$。

当 $j=k+1$ 时，那么 $q_a \overset{k+1}{\not\sim} q_b$，但 $q_a \overset{k}{\sim} q_b$，与 $P_k=P_{k+1}$ 矛盾。

当 $j>k+1$ 时，因为 $q_a \overset{j}{\nsim} q_b$，必存在一个长度为 j 的字符串 ω，其中 $\omega=\varphi\psi$，$|\psi|=k+1$，$|\varphi|=|\omega|-|\psi|=j-(k+1)\geqslant 1$，即 φ 非空，使得

$$O(q_a,\ \varphi\psi)\neq O(q_b,\ \varphi\psi)$$

即
$$O(f(q_a,\ \varphi),\ \psi)\neq O(f(q_b,\ \varphi),\ \psi)$$

令 $q_a'=f(q_a,\ \varphi)$，$q_b'=f(q_b,\ \varphi)$，那么 $q_a' \overset{k+1}{\nsim} q_b'$。但对于任意长度不超过 k 的字符串 μ，

$$|\varphi\mu|=|\varphi|+|\mu|\leqslant j-(k+1)+k=j-1$$

因为 j 是使 q_a 与 q_b 不是 j 等价的最小正整数，所以 $q_a \overset{j-1}{\sim} q_b$，

$$O(q_a,\ \varphi\mu)=O(q_b,\ \varphi\mu)$$

即
$$O(f(q_a,\ \varphi),\ \mu)=O(f(q_b,\ \varphi),\ \mu)$$

$$O(q_a',\ \mu)=O(q_b',\ \mu)$$

因此，$q_a' \overset{k}{\sim} q_b'$，与 $P_k=P_{k+1}$ 矛盾。 □

对状态集 Q 构造等价划分 P，首先要构成 P_1，然后由 P_1 构造 P_2，P_2 构造 P_3，…，直到 $P_k=P_{k+1}$ 为止。为了由 P_i 构造 P_{i+1}，我们给出下列定理。

定理 8-5.3 设 $q_a,\ q_b\in Q$，那么，$q_a \overset{k+1}{\sim} q_b$ 的充要条件是 $q_a \overset{k}{\sim} q_b$，且对所有输入字母 $s\in S$，有 $f(q_a,\ s) \overset{k}{\sim} f(q_b,\ s)$。

证明　因为 $q_a \overset{k+1}{\sim} q_b$ 必有 $q_a \overset{k}{\sim} q_b$。此外，对所有长度不超过 $k+1$ 的字符串 $s\omega\in S^*$，其中 $s\in S$，$\omega\in S^*$，$|\omega|\leqslant k$，有

$$O(q_a,\ s\omega)=O(q_b,\ s\omega)$$

即
$$O(f(q_a,\ s),\ \omega)=O(f(q_b,\ s),\ \omega)$$

因此
$$f(q_a,\ s) \overset{k}{\sim} f(q_b,\ s)$$
□

充分性的证明留作习题。

例题 1　给定有限状态机

$M=(\{A,\ B,\ C,\ D,\ E,\ F,\ G,\ H,\ J\},\ \{0,\ 1\},\ \{0,\ 1\},\ f,\ g,\ q_I)$

它的状态表如表 8-5.1 所示。

表 8-5.1

	0	1
A	B, 0	C, 0
B	C, 1	D, 1
C	D, 0	E, 0
D	C, 1	B, 1
E	F, 1	E, 1
F	G, 0	C, 0
G	F, 1	G, 1
H	J, 1	B, 0
J	H, 1	D, 0

构造等价划分 P。

解　从表 8-5.1 知道

$$g(A, 0)=g(C, 0)=g(F, 0)=0$$

$$g(A, 1)=g(C, 1)=g(F, 1)=0$$

$$A \overset{1}{\sim} C \overset{1}{\sim} F$$

$$g(B, 0)=g(D, 0)=g(E, 0)=g(G, 0)=1$$

$$g(B, 1)=g(D, 1)=g(E, 1)=g(G, 1)=1$$

$$B \overset{1}{\sim} D \overset{1}{\sim} E \overset{1}{\sim} G$$

$$g(H, 0)=g(J, 0)=1$$

$$g(H, 1)=g(J, 1)=0$$

$$H \overset{1}{\sim} J$$

$$P_1=\{\{A, C, F\}, \{B, D, E, G\}, \{H, J\}\}$$

因为 $f(A, 0)=B$, $f(C, 0)=D$, $f(F, 0)=G$, 它们都在 P_1 的同一等价类中，而 $f(A, 1)=f(F, 1)=C$, $f(C, 1)=E$, 状态 A, F 的 1-后继在 P_1 的同一等价类中，而状态 C 的 1-后继在 P_1 的另一等价类中，因此 P_1 中的等价类 $\{A, C, F\}$ 应加细为 $\{A, F\}$ 和 $\{C\}$。

状态 B, D, E, G 的 0-后继都在 P_1 的等价类 $\{A, C, F\}$ 中，1-后继都在 P_1 的等价类 $\{B, D, E, G\}$ 中，所以，它们仍在 P_2 的同一等价类中。

状态 H, J 的 0-后继都在 P_1 的等价类 $\{H, J\}$ 中，1-后继都在 P_1 的等

价类 $\{B, D, E, G\}$ 中，所以，不再需要加细。因此

$$P_2=\{\{A, F\}, \{C\}, \{B, D, E, G\}, \{H, J\}\}$$

同理可得 $$P_3=\{\{A, F\}, \{C\}, \{B, D\}, \{E, G\}, \{H, J\}\}$$

$$P_4=\{\{A\}, \{F\}, \{C\}, \{B, D\}, \{E, G\}, \{H, J\}\}$$

$$P_5=P_4$$

因此 $$P=\{\{A\}, \{F\}, \{C\}, \{B, D\}, \{E, G\}, \{H, J\}\}$$

例题 2 对于上例中状态 A, F, 构造有不同响应的激励。

解 状态 A 和 F 在 P_4 的不同等价类中，所以可设它们有不同响应的激励是 $s(1)s(2)s(3)s(4)$。

1. 状态 A 和 F 的 $s(1)$-后继必在 P_3 的不同等价类中，只能取 $s(1)=0$，且 $A \xrightarrow{0/0} B$, $F \xrightarrow{0/0} G$。

2. 状态 B 和 G 的 $s(2)$-后继必须在 P_2 的不同等价类中，只能取 $s(2)=0$，且 $B \xrightarrow{0/1} C$, $G \xrightarrow{0/1} F$。

3. 状态 C 和 F 的 $s(3)$-后继必须在 P_1 的不同等价类中，只能取 $s(3)=1$，且 $C \xrightarrow{1/0} E$, $F \xrightarrow{1/0} C$。

4. 状态 E 和 C 必须对应不同的输出，因为 $g(E, 0)=1$, $g(C, 0)=0$; $g(E, 1)=1$, $g(C, 1)=0$, 可取 $s(4)=0$ 或 $s(4)=1$。

因而有不同响应的激励是

$$\omega_1=0010 \quad 或 \quad \omega_2=0011$$

对于 $\omega_1=0010$，有

$$A \xrightarrow{0/0} B \xrightarrow{0/1} C \xrightarrow{1/0} E \xrightarrow{0/1} F$$

$$F \xrightarrow{0/0} G \xrightarrow{0/1} F \xrightarrow{1/0} C \xrightarrow{0/0} D$$

所以，从状态 A 出发，响应是 0101，从状态 F 出发，响应是 0100。

对于 $\omega_2=0011$，有

$$A \xrightarrow{0/0} B \xrightarrow{0/1} C \xrightarrow{1/0} E \xrightarrow{1/1} E$$

$$F \xrightarrow{0/0} G \xrightarrow{0/1} F \xrightarrow{1/0} C \xrightarrow{1/0} E$$

所以，从状态 A 出发，响应是 0101，从状态 F 出发，响应是 0100。由此可知，有不同响应的激励不是唯一的。

有了上面一些结果，就可以将一台有限自动机简化。

定义 8-5.4 给定一台有限状态机 $M=(Q, S, R, f, O, q_I)$，如果对于任意 q_a, $q_b \in Q$，当 $q_a \sim q_b$ 时，必有 $q_a = q_b$，就称 M 是简化机。

在简化机 M 中，不存在不同的等价状态，因此，简化机的 P 划分中每一等价类只含一个状态。

给定一台有限状态机 M，希望构造一台等价的简化机 M'，我们可以这样进行：M' 的状态对应机器 M 的划分 P 中一个等价类，M' 的初态对应机器 M 的划分 P 中含有 M 初态的等价类。M' 的输入字母表，输出字母表分别与 M 的输入字母表，输出字母表相同。M' 的状态表由下面两条规则得到：

1. 为了找 M' 中状态 q' 的 s-后继，先在机器 M 的划分 P 中找出对应 q' 的等价类，在此等价类中任取一状态，求出此状态的 s-后继，而包含此 s-后继的等价类所对应的 M' 中的状态，就是 q' 的 s-后继。

2. 对于转换赋值机，状态 q' 的 s 转换输出就是对应 q' 的等价类中任一状态的 s 转换输出。

对于状态赋值机，状态 q' 的输出是对应 q' 的等价类中任一状态的输出。

例题 8 构造与例题 1 中的转换赋值机等价的简化机。

解 (a) P: $\{A\}$, $\{F\}$, $\{C\}$, $\{B, D\}$, $\{E, G\}$, $\{H, J\}$

M' 中的新名: U　V　W　X　Y　Z

(b)

新名	等价类	0	1
U	$\{A\}$	$\{B\}$, 0	$\{C\}$, 0
V	$\{F\}$	$\{G\}$, 0	$\{C\}$, 0
W	$\{C\}$	$\{D\}$, 0	$\{E\}$, 0
X	$\{B, D\}$	$\{C\}$, 1	$\{D, B\}$, 1
Y	$\{E, G\}$	$\{F\}$, 1	$\{E, G\}$, 1
Z	$\{H, J\}$	$\{J, H\}$, 1	$\{B, D\}$, 0

(c) M':

	0	1
U	X, 0	W, 0
V	Y, 0	W, 0
W	X, 0	Y, 0
X	W, 1	X, 1
Y	V, 1	Y, 1
Z	Z, 1	X, 0

8-5 习题

(1) 完成定理8-5.3的证明。

(2) 证明，如果有限自动机 M 有 n 个状态，其中 $n\geqslant 2$，则存在一个整数 $k\leqslant n-1$，使得 $P_k=P$。

(3) 设 M 是有 n 个状态的有限状态机，q 是 M 中一个状态。如有一个激励 ω，使 $f(q_I, \omega)=q$，则必有 $\omega'\in S^*$，$|\omega'|\leqslant n-1$，使 $f(q_I, \omega')=q$。

(4) 试简化（如果有可能）转换赋值机 M，它的状态如表8-5.2所示。

表 8-5.2

	0	1
s_0	s_1, 0	s_7, 0
s_1	s_7, 0	s_0, 1
s_2	s_3, 0	s_1, 1
s_3	s_7, 0	s_5, 1
s_4	s_3, 0	s_2, 0
s_5	s_6, 0	s_7, 0
s_6	s_8, 0	s_5, 1
s_7	s_2, 0	s_7, 1
s_8	s_2, 0	s_0, 1

(5) 简化转换赋值机 M，它的状态表如表8-5.3所示。

表 8-5.3

	a	b	c	d
s_0	s_4, 1	s_2, 0	s_1, 1	s_4, 1
s_1	s_2, 0	s_5, 1	s_4, 1	s_1, 0
s_2	s_1, 1	s_0, 0	s_3, 1	s_5, 1
s_3	s_6, 0	s_5, 1	s_4, 1	s_1, 0
s_4	s_2, 0	s_5, 1	s_3, 1	s_4, 0
s_5	s_2, 1	s_5, 1	s_3, 0	s_7, 0
s_6	s_3, 1	s_0, 0	s_1, 1	s_5, 1
s_7	s_1, 1	s_2, 0	s_4, 1	s_5, 1

画出简化机的状态图，对于状态 s_0, s_7, 求出有不同响应的激励。

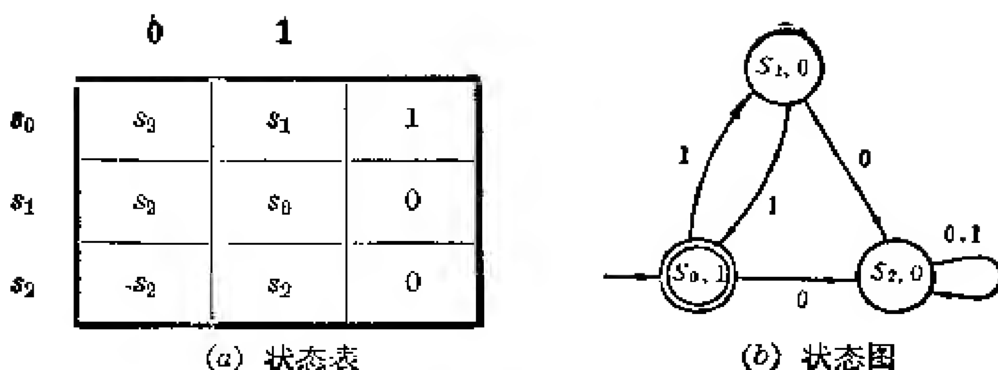
(6) 证明，如果 $P_k \neq P$, 则 $|P| \geq k+2$。

8-6 有限状态机与正则语言

给定有限状态机 $M=(Q, S, R, f, O, q_I)$，对于任一激励 $\omega \in S^+$，能产生一个响应 $r \in R^+$，因此，M 就是一台将输入字符串 ω 转换为输出字符串 r 的转换器。如果给定 S 上一个语言 L，为了判别任一输入字符串 ω 是否在 L 中，只要考察 $O(q_I, \omega)$，约定当 $\omega \in L$ 时，$O(q_I, \omega)=1$，当 $\omega \notin L$ 时，$O(q_I, \omega)=0$。由于 $O(q_I, \omega)$ 与 q_I 的 ω-后继状态有关，因此可在状态集 Q 中构造一个子集 F，使得当 $\omega \in L$ 时，$f(q_I, \omega) \in F$，$O(q_I, \omega)=1$；当 $\omega \notin L$ 时，$f(q_I, \omega) \notin F$ 时，$O(q_I, \omega)=0$；这样就可用 q_I 的 ω-后继是否在 F 中来判别 ω 是否在 L 中，这个状态子集 F 称为终态集，其中每一状态称为终态，在状态图中用双圈来表示。至此，有限状态机 M 可看成一台语言 L 的识别器。

例 1　给定有限状态机 M_1，它的状态表如图 8-6.1(a)所示，状态图如图 8-6.1(b)所示，终态集 $F=\{S_0\}$。

显然，当 $\omega=(11)^*$ 时，$f(S_0, \omega)=S_0 \in F$，反之亦然。故 M_1



	0	1	
s_0	s_2	s_1	1
s_1	s_2	s_0	0
s_2	s_2	s_2	0

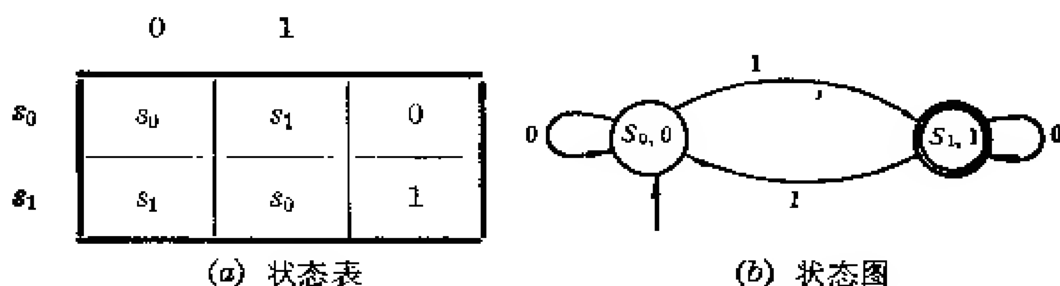
(a) 状态表　　(b) 状态图

图 8-6.1

接受的语言为

$$L_1=\{(11)^n \mid n\geqslant 0\}$$

例 2　给定有限状态机 M_2，它的状态表如图 8-6.2(a)所示，状态图如图 8-6.2(b)所示，终态集 $F=\{S_1\}$。



	0	1	
s_0	s_0	s_1	0
s_1	s_1	s_0	1

(a) 状态表　　(b) 状态图

图 8-6.2

显然，当 $\omega=(0^*10^*1)^*0^*10^*$ 时，$f(S_0, \omega)=S_1\in F$，因此 M_2 接受的语言 L_2 是由那些含有奇数个 1 的二进制串所组成。

在上述两例中，可以看到 R, O 对判别 ω 是否属于 L 无关紧要，但 F 却起决定作用。

定义 8-6.1　一个有限状态接收器是五有序组

$$M=(Q,\ S,\ \delta,\ I,\ F)$$

其中：Q 是有限状态集；

S 是有限输入字母集；

$I\subseteq Q$ 是初态集；

$F\subseteq Q$ 是终态集；

δ 是 $Q\times S\to Q$ 的关系，称为 M 的转换关系，当 $q'\in\delta(q, s)$ 时，就有

$$q \xrightarrow{*} q'$$

定义 8-6.2 给定有限状态接收器 $M=(Q, S, \delta, I, F)$，若存在 $q_I \in I$，使得

$$\delta(q_I, \omega) \cap F \neq \emptyset$$

则称 ω 被 M 接受。所有被 M 接受的输入字符串所组成的集合称为 M 可接受的语言，记为 $L(M)$。

例 3 有限状态接收器 M_3 的状态图如图 8-6.3 所示。

其中：

$$Q=\{A, B, C\}$$
$$I=\{A\}$$
$$F=\{C\}$$
$$S=\{0, 1\}$$
$$\delta(A, 0)=\{A, C\},\ \delta(A, 1)=\{B\}$$
$$\delta(B, 0)=\{C\},\ \delta(B, 1)=\emptyset,\ \delta(C, 0)=\emptyset$$
$$\delta(C, 1)=\{C\}$$

M_3 接受的语言是

$$L(M_3)=\{0^*01^*, 0^*101^*\}$$

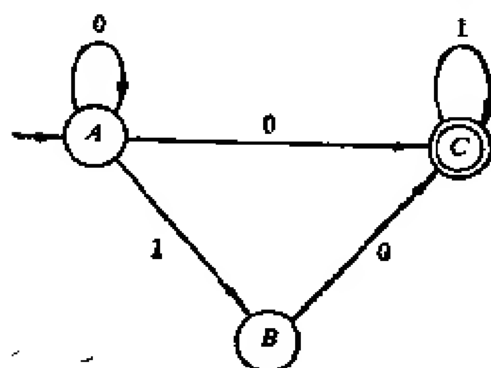


图 8-6.3

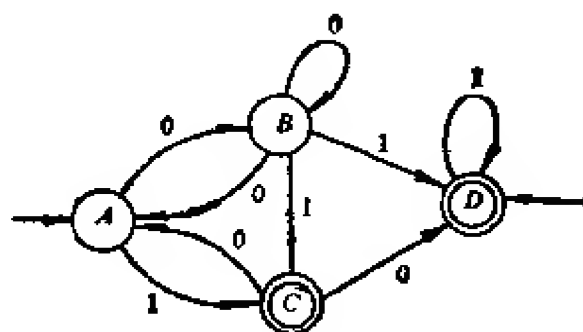


图 8-6.4

例 4 有限状态接收器 M_4 的状态图如图 8-6.4 所示。

其中：

$$Q=\{A, B, C, D\}$$
$$I=\{A, D\}$$
$$F=\{C, D\}$$
$$S=\{0, 1\}$$
$$\delta(A, 0)=\{B\},\ \delta(A, 1)=\{C\},\ \delta(B, 0)=\{A, B\}$$

$\delta(B, 1)=\{C, D\}$, $\delta(C, 0)=\{A, D\}$, $\delta(C, 1)=\emptyset$

$\delta(D, 0)=\emptyset$, $\delta(D, 1)=\{D\}$

显然　　$L(M_4)=\{1, 1000^*1, 00^*11^*, 00^*101^*, \cdots\}$。

我们从例 3 和例 4 可以看到有限状态接收器和有限状态机有下面三点不同：

1. 有限状态机的初态只是一个状态 q_I，而有限状态接收器有一个非空初态集，其中每一状态都可作为初态。

2. 对于有限状态机我们主要考虑对于激励 ω 的响应，而有限状态接收器我们考虑的是对于激励 ω 的后继是否在终态集中，以便决定此激励是否被接受。

3. 有限状态机中 f 是 $Q\times S\to Q$ 的一个状态转换函数，因此对于任一 $q\in Q$, $s\in S$ 都有唯一的 q'，使 $q\xrightarrow{s}q'$，这种转换称为是确定的转换。

有限状态接收器中，δ 是 $Q\times S\to Q$ 的一个状态转换关系，故可以有 $q\in Q$, $s\in S$，使得 $q\xrightarrow{s}q_1'$, $q\xrightarrow{s}q_2'$, $\cdots$, $q\xrightarrow{s}q_k'$ $(k\geqslant 1)$，此时 $\delta(q, s)=\{q_1', q_2', \cdots, q_k'\}$。另外，还可能有 $q\in Q$, $s\in S$，使得 q 的 s-后继不存在，此时 $\delta(q, s)=\emptyset$。这些转换都称为不确定的转换。

如例 3 中有 $\delta(A, 0)=\{A, C\}$, $\delta(B, 1)=\delta(C, 0)=\emptyset$。例 4 中有 $\delta(B, 0)=\{A, B\}$, $\delta\{B, 1\}=\{C, D\}$, $\delta(C, 0)=\{A, D\}$, $\delta(C, 1)=\delta(D, 0)=\emptyset$。

定义 8-6.3　有限状态接收器 $M=(Q, S, \delta, I, F)$，如果 δ 是 $Q\times S\to Q$ 的一个函数且 I 集合中只有一个状态，称 M 是确定的有限状态接收器。否则，称 M 是不确定的有限状态接收器。

例 1 和例 2 是确定的有限状态接收器，例 3 和例 4 是不确定的有限状态接收器。

确定的有限状态接收器是不确定的有限状态接收器的特殊情形。反之，我们有下列定理。

定理 8-6.1　对每一台有限状态接收器 M，可以构造一台确

定的有限状态接收器 M'，使 $L(M)=L(M')$。

这个定理，我们不再证明[注]。 □

下面我们讨论3型文法产生的正则语言与由有限状态接收器所接受的语言之间的关系。

定理 8-6.2 设 $G=(V_N, V_T, P, \sigma)$ 是一个3型文法，则存在一台有限状态接收器 $M=(Q, S, \delta, I, F)$，使得

$$L(M)=L(G)$$

证明 只对 G 是右线性文法加以证明。当 G 是左线性文法时，可以类似证明。

令 M 的输入字母集 $S=V_T$。M 中的状态集 $Q=V_N\cup\{A\}$。其中 $A\notin V_N$。M 的初始状态集 $I=\{\sigma\}$。如果 G 的生成式中含有 $\sigma\to\lambda$，则 M 的终态集 $F=\{\sigma, A\}$，否则 $F=\{A\}$。我们这样来构造 δ，如果在 G 的生成式中含有 $B\to a$，那么，就有 $A\in\delta(B, a)$。如果在 G 的生成式中含有 $B\to aC$，那么，就有 $C\in\delta(B, a)$。

对所有 $a\in V_T$，令 $\delta(A, a)=\emptyset$。这样构造出来的有限状态接收器 M，一般将是不确定的。下面我们证明

$$L(M)=L(G)$$

设 $\omega\in L(G)$，$\omega=a_1a_2\cdots a_n$，$(n\geqslant1)$，那么，在 $L(G)$ 中有某个非终结符序列 $A_1, A_2, \cdots, A_{n-1}$，使得 $\sigma\Rightarrow a_1A_1\Rightarrow a_1a_2A_2\Rightarrow\cdots\Rightarrow a_1a_2\cdots a_{n-1}A_{n-1}\Rightarrow a_1a_2\cdots a_{n-1}a_n$，从 δ 的构造，可知

$$A_1\in\delta(\sigma, a_1),\ A_2\in\delta(A_1, a_2),\ \cdots,\ A\in\delta(A_{n-1}, a_n)$$

因为 $A\in F$，即 σ 的 ω-后继在 F 中，而此 $\omega\in L(M)$。

如果 $\omega=\lambda\in L(G)$，则在 P 中，有生成式 $\sigma\to\lambda$，因此，$\sigma\in F$，即 σ 的 λ-后继也在 F 中，因此 $\lambda\in L(M)$。

综上所述，有

$$L(G)\subseteq L(M)$$

设 $\omega=a_1a_2\cdots a_n\in L(M)$，$n\geqslant1$，即 S 的 ω-后继在 F 中，于是，存在状态序列 $\sigma, A_1, A_2, \cdots, A_{n-1}$，使得 $A_1\in\delta(\sigma, a_1)$，

[注] 参阅 Peter J. Denning, Jack B. Dennis, Joseph E. Qualitz: Machines, Languages and Computation p. 145。

$A_2 \in \delta(A_1, a_2)$, …, $A_{n-1} \in \delta(A_{n-2}, a_{n-1})$, $A \in \delta(A_{n-1}, a_n)$。所以，$P$ 中有生成式 $\sigma \to a_1 A_1$, $A_1 \to a_2 A_2$, …, $A_{n-1} \to a_n$，因此

$$S \Rightarrow a_1 A_1 \Rightarrow a_1 a_2 A_2 \Rightarrow \cdots \Rightarrow a_1 a_2 \cdots a_{n-1} A_{n-1} \Rightarrow a_1 a_2 \cdots a_{n-1} a_n$$

$$\omega \in L(G)$$

如果 $\omega = \lambda \in L(M)$，则 $\sigma \in F$，即 P 中有生成式 $\sigma \to \lambda$，因此，$\sigma \Rightarrow \lambda$，$\lambda \in L(G)$。

综上所述，有

$$L(M) \subseteq L(G)$$

因此
$$L(M) = L(G)$$
□

例题 1 给定正则文法 $G = (\{\sigma, B\}, \{0, 1\}, P, \sigma)$，其中 P 含有:

$$\sigma \to 0B,\ B \to 0B,\ B \to 1\sigma,\ B \to 0$$

试构造一台接受相同语言的有限状态接收器，并画出状态图。

解 令 $M = (Q, S, \delta, I, F)$，其中 $Q = \{\sigma, B, A\}$，$S = \{0, 1\}$，$I = \{\sigma\}$，$F = \{A\}$，δ 定义如下:

1. 因为 $\sigma \to 0B$ 是 σ 在左边，0 在右边的 P 中的唯一生成式，故
$$\delta(\sigma, 0) = \{B\}$$
2. 因为 P 中不包含 σ 在左边，1 在右边的生成式，故 $\delta(\sigma, 1) = \emptyset$。
3. 因为 $B \to 0B$ 和 $B \to 0$ 都在 P 中，故 $\delta(B, 0) = \{B, A\}$。
4. 因为 $B \to 1\sigma$ 是 B 在左边，1 在右边的 P 中的唯一生成式，故
$$\delta(B, 1) = \{\sigma\}$$
5. $\delta(A, 0) = \delta(A, 1) = \emptyset$。

M 的状态图如图 8-6.5 所示。

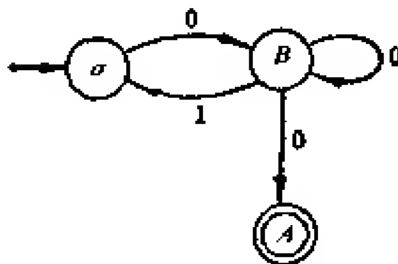


图 8-6.5

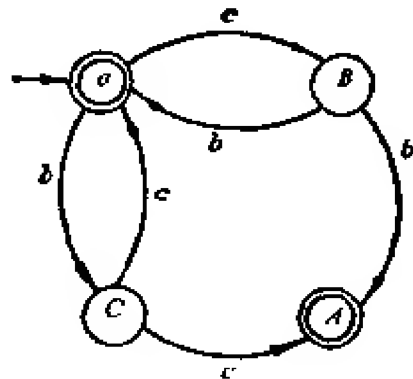


图 8-6.6

例题 2 给定正则文法 $G = (\{\sigma, B, C\}, \{b, c\}, P, \sigma)$，其中 P 含有:

$$\sigma \to bC,\ \sigma \to cB,\ \sigma \to \lambda,\ B \to b\sigma,\ C \to c\sigma,\ B \to b,\ C \to c$$

试构造一台接受相同语言的有限状态接收器，并画出状态图。

解　令 $M=(Q, S, \delta, I, F)$，其中

$$Q=\{\sigma, B, C, A\},\ S=\{b, c\},\ I=\{\sigma\}$$

因为 P 中含有生成式 $\sigma\to\lambda$，所以 $F=\{\sigma, A\}$。δ 定义如下：

1. 因为 P 中含有 $\sigma\to bC$，所以 $\delta(\sigma, b)=\{C\}$。
2. 因为 P 中含有 $\sigma\to cB$，所以 $\delta(\sigma, c)=\{B\}$。
3. 因为 P 中含有 $B\to b\sigma$，$B\to b$，所以 $\delta(B, b)=\{\sigma, A\}$。
4. 因为 P 中含有 $C\to c\sigma$，$C\to c$，所以 $\delta(C, c)=\{\sigma, A\}$。
5. $\delta(A, b)=\delta(A, c)=\emptyset$。

M 的状态图如图 8-6.6 所示。

定理 8-6.3　设 $M=(Q, S, \delta, I, F)$ 是一台有限状态接收器，则存在一个 3 型文法 G，使 $L(G)=L(M)$。

证明　我们构造一个右线性文法 G，使 $L(G)=L(M)$。也可类似地构造一个左线性文法 G，使 $L(G)=L(M)$。

令 $G=(V_N, V_T, P, \sigma)$，这里 V_T 是 M 的输入字母集 S。

(1) 当 I 只包含一个状态时：将 M 的初态作为 G 的初始符 σ，M 的状态集 Q 作为 G 的非终结符集 V_N，且 P 是这样来构造：

1. 若 $\delta(B, a)=\{C_1, C_2, \cdots, C_k\}$，则 P 中含有生成式

$$B\to aC_1,\ B\to aC_2,\ \cdots,\ B\to aC_k$$

2. 若 $C_i\in\delta(B, a)$，且 $C_i\in F$，则 P 中含有生成式 $B\to a$。
3. 如果 $I\cap F\neq\emptyset$，则 P 中含有生成式 $\sigma\to\lambda$。

(2) 当 I 包含多个状态时：

我们增加一个不在 Q 中的字符 σ，作为 G 的初始符。P 的构造与上面类似，同时再增加下列生成式 $\sigma\to A$，这里 $A\in I$。

由上述方法构成的文法，还不是右线性文法，因为对任意初态 A，有生成式 $\sigma\to A$。为了构造生成相同语言的右线性文法，我们将形如 $\sigma\to A$ 生成式删去，并在剩下的生成式中，将所有出现初态 A 的地方用 σ 代替，这样所得的文法就是所需的右线性文法，这里 $V_N=(Q-I)\cup\{\sigma\}$。

我们可以用与证明定理 8-6.2 一样的方法来证明它，留作习题。□

例题 3 给定有限状态接收器

$$M=(\{S_0, S_1\}, \{a, b\}, \delta, \{S_0\}, \{S_1\})$$

其中

$$\delta(S_0, a)=\{S_0\}$$
$$\delta(S_0, b)=\{S_1\}$$
$$\delta(S_1, a)=\{S_1\}$$
$$\delta(S_1, b)=\{S_0\}$$

试构造一个右线性文法 G，使 $L(G)=L(M)$。

解 令 $G=(V_N, V_T, P, \sigma)$，则 $V_T=\{a, b\}$。因为 I 中只包含一个状态 S_0，所以，取 S_0 作为 σ。

$V_N=\{S_0, S_1\}$，构造 P：

1. 因为 $\delta(S_0, a)=\{S_0\}$，所以 P 中有生成式 $S_0\to aS_0$。

2. 因为 $\delta(S_0, b)=\{S_1\}$ 且 $S_1\in F$，所以，P 中有生成式

$$S_0\to bS_1, \quad S_0\to b$$

3. 因为 $\delta(S_1, a)=\{S_1\}$ 且 $S_1\in F$，所以，P 中有生成式

$$S_1\to aS_1, \quad S_1\to a$$

4. 因为 $\delta(S_1, b)=\{S_0\}$，所以，P 中有生成式 $S_1\to bS_0$。

因此 P：
$$S_0\to aS_0,\ S_0\to bS_1,\ S_0\to b$$
$$S_1\to aS_1,\ S_1\to bS_0,\ S_1\to a$$

例题 4 给定有限状态接收器

$$M=(\{S_0, S_1, S_2\}, \{0, 1\}, \delta, \{S_0, S_1\}, \{S_0\})$$

其中

$$\delta(S_0, 0)=\{S_2\}$$
$$\delta(S_0, 1)=\{S_0, S_1\}$$
$$\delta(S_1, 0)=\{S_2\}$$
$$\delta(S_2, 0)=\{S_0, S_1\}$$
$$\delta(S_2, 1)=\{S_2\}$$

试构造一个右线性文法 G，使 $L(G)=L(M)$。

解 令 $G=(V_N, V_T, P, \sigma)$，则 $V_T=\{0, 1\}$；因为 I 包含两个状态 S_0 和 S_1，引进字符 $\sigma\notin Q$ 作为 G 的初始符，生成式 P 这样来构造：

1. 由 δ 可知，P 中含有 $S_0\to 0S_2$, $S_0\to 1S_0$, $S_0\to 1$, $S_0\to 1S_1$, $S_1\to 0S_2$, $S_2\to 0S_0$, $S_2\to 0$, $S_2\to 0S_1$, $S_2\to 1S_2$。

2. 因为 $S_0\in I$, $S_0\in F$，所以，P 中含有 $\sigma\to\lambda$。

3. P 中还含有生成式 $\sigma\to S_0$, $\sigma\to S_1$。

4. 删去 $\sigma\to S_0$, $\sigma\to S_1$，将余下的生成式中出现 S_0 和 S_1 的地方换为 σ，则可得 P 为：

$$\sigma\to 0S_2,\ \sigma\to 1\sigma,\ \sigma\to 1,\ S_2\to 0\sigma,\ S_2\to 0,\ S_2\to 1S_2,\ \sigma\to\lambda$$

8-6 习题

(1) 给定有限状态接收器，$M=(Q, S, \delta, I, F)$的状态图

a)

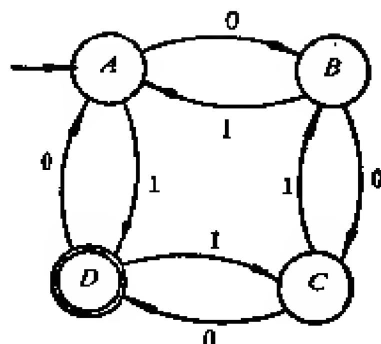


图 8-6.7

b)

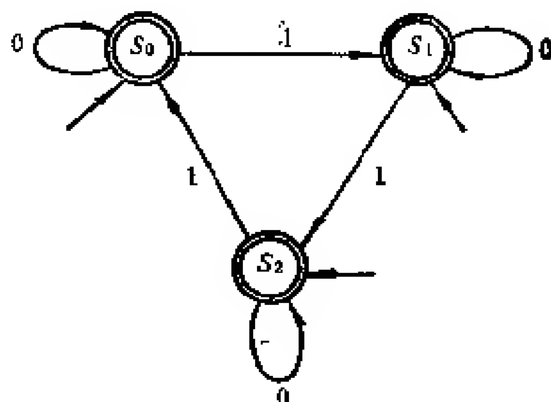


图 8-6.8

c)

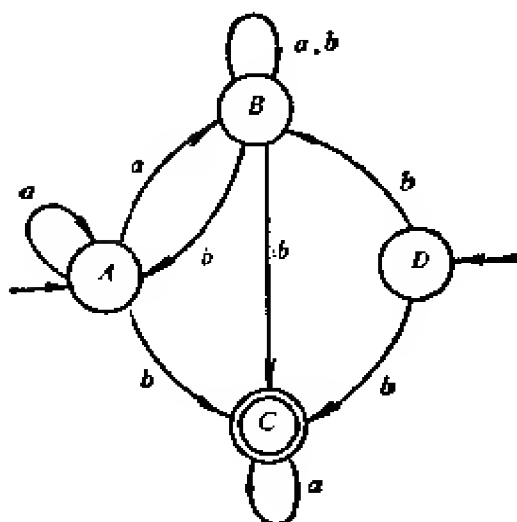


图 8-6.9

分别写出 Q, S, δ, I, F, 说明它们是确定的还是不确定的。

(2) 写出下列有限状态接收器接受的语言。

a)

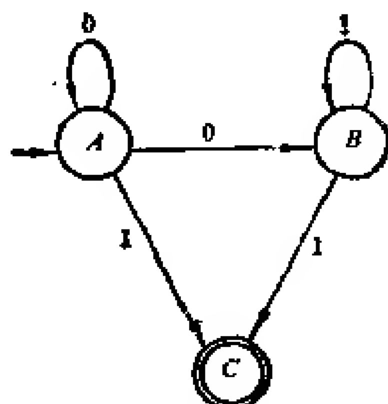


图 8-6.10

b)

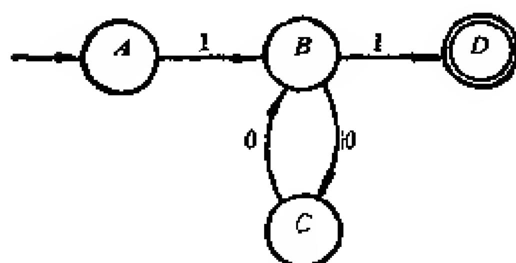


图 8-6.11

(3) 完成定理 8-6.3 的证明。

(4) 对于图 8-6.12 所示的有限状态接收器 M，构造文法 G，使

$$L(G)=L(M)$$

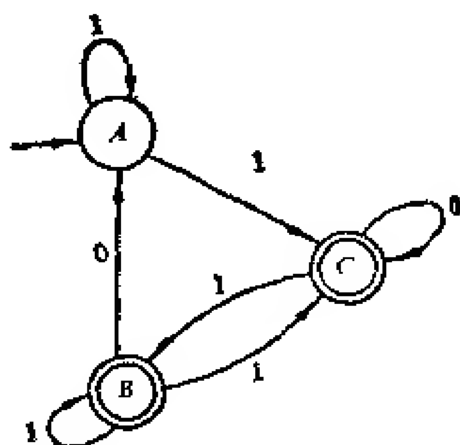


图 8-6.12

(5) 给定正则文法 $G=(\{0,1\},\{\sigma,A,B\},P,\sigma)$，其中

$$P:\ \sigma\to 1A,\ A\to 1B,\ B\to 1B,\ B\to 0\sigma,\ B\to 0$$

试描述 $L(G)$并给出接受该语言的有限状态接收器。

第九章　纠错码初步

纠错编码技术是五十年代提出，六十年代发展起来的。近来，由于数字通讯，特别是卫星通讯的发展，以及在数字计算机和数据处理等新兴科学技术中广泛应用，给纠错码开拓了新的发展前景。

本章主要讨论线性分组码，并给出构造能纠单错的群码的方法。

9-1　通讯模型和纠错的基本概念

人类社会中，为了加强交往，需要交换各种信息，于是产生了交换信息的各种方法，例如写一封信，通一次电话，发一份电报，通过广播等多种手段。上述这些通讯方法，除了写信外，其它三种通讯手段都要经过三个必要步骤：

1．在发送端将所要传送的信息转换成电信号。

2．通过可靠的信道，传输电信号。

3．在接收端将接收到的电信号还原成原来的信息。

电信号可分为模拟信号和数字信号两种。例如电话机话筒输出的电压，其幅值随说话人的语言连续变化，它与信息直接对应，且可取无限多个值，这种信号称为模拟信号。又如电报，是以四个数字代表一个汉字，且代表每个数字的脉冲信号，其高度只取两个值分别表示空号和传号，（通常用0和1表示）这种信号不仅在取值上有限和离散，而且在时间上也是离散的，它称为离散信号或数字信号。这里，我们限于讨论数字信号。

在现代数字通讯系统和计算机中，信号都采用二进制，即用一个由“0”或“1”组成的符号串来表示传输的信息。例如，五位二进

制：00000，00001，00010，…，11111 可表示 32 个不同的符号，因此，26 个英文字母及六个附加的必要符号就可用它们来表示。例如，"北京"的拼音"*BEIJING*"，其电传码是：

10011(B)，10000(E)，01100(I)，11010(J)，
01100(I)，00110(N)，01011(G)

"北京"的英语"*PEKING*"，其电传码为：

01101(P)，10000(E)，11110(K)，01100(I)
00110(N)，01011(G)

表 9-1.1 给出了五单位电传码和 3:4 等重码。

表 9-1.1

号码	字母	5 单位码	3:4 码
—	A	11000	0011010
?	B	10011	0011001
:	C	01110	1001100
你是谁	D	10010	0011100
3	E	10000	0111000
%	F	10110	0010011
‰	G	01011	1100001
	H	00101	1010010
8	I	01100	1110000
ℜ	J	11010	0100011
(	K	11110	0001011
)	L	01001	1100010
.	M	00111	1010001
,	N	00110	1010100
9	O	00011	1000110
0	P	01101	1001010
1	Q	11101	0001101
4	R	01010	1100100
'	S	10100	0101010
5	T	00001	1000101
7	U	11100	0110010
=	V	01111	1001001
2	W	11001	0100101
/	X	10111	0010110
6	Y	10101	0010101
"	Z	10001	0110001
回行〉		00010	1000011
换行≡		01000	1011000
字母键		11111	0100110
数学键		11011	0001110
间　隔		00100	1101000
		00000	0000111
RQ			0110100
α			0101001
β			0101100

下面讨论信息传输中纠错的概念。

一个典型的通讯系统模型如图 9-1.1 所示。

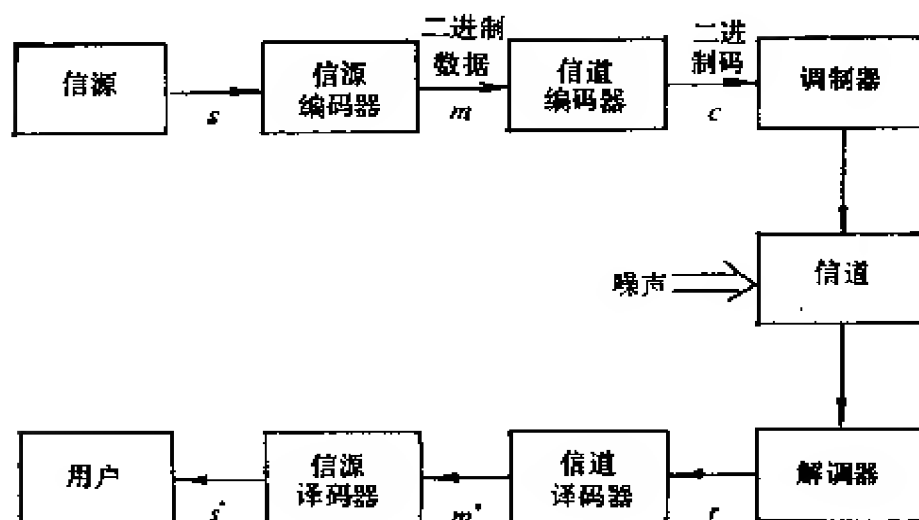


图 9-1.1

此系统的第一单元是信源，它可以是人或机器(例如电子计算机)。信源的输出可以是一个连续波形，或者是离散的符号序列。信源编码器将信源的输出信号 s 变换成二进制序列 m，它称为信息序列。信道编码器将信息序列 m 变换成比 m 更长的二进制序列 c，c 称为码字。二进制码不能在实际信道上传输，调制器将二进制码 c 的每位数字编码成持续时间为 T 的正、负脉冲。调制器输出信号通过信道传输并被噪声干扰。解调器对每个持续时间为 T 的换收信号进行判决，以确定发送的是 1 还是 0。于是，解调器的输出是二进制序列 r，r 称为接收序列。由于信道噪声的干扰，接收序列 r 与码字 c 可能不一致。例如，若发送的是 $c=000110$，收到的是 $r=100010$，那么，在第一位和第四位发生了错误。信道译码器就是要试图纠正 r 中的传输错误，并产生真正发送的码字 c 的估值 c^*，并将 c^* 转换为 m 的估值 m^*。而信源译码器将 m^* 转换成真正信源输出 s 的估值 s^*，并送至用户。如果信道无噪声干扰，则 c^*，m^*，s^* 分别是 c，m，s 的重现。如果噪声很大，s^* 可能与真正信源输出 s 差别十分大。

数字通信中一个重要的问题是设计信道的编码器——译码器

对，使得信道译码器的输出端能够可靠地重现信息序列 m。信道编码器通常是将信源编码器输出的二进制数据 m 变换成一个更长的二进制码，使它具备对付噪声干扰的能力，上述设计方法的根据是1948年Shannon所提出的编码定理。该定理指出，在一定的条件下，只要码的长度充分大时，一定存在一种编码、译码方法，使得错误译码的概率充分小。

定义 9–1.1 任一由0,1字母组成的字符串称为字。一些字的集合称为码。码中的字称为码字，不在码中的字称为废码。码字中的每一个字母0或1称为码元。

例如，长度为2的字集 $S_2=\{00, 01, 10, 11\}$ 有 2^2 个不同的字，它们可用一个正方形表示，如图 9–1.2(*a*)所示。其中，每一个字占据正方形的一个顶点，两个字之间如果只有一个字母不同，它们就在一条边的两端。两个字如果两个字母都不同，它们就在对角线的两端，反之亦然。由此可知，两个字中不同字母的个数恰等于从一个字出发沿着正方形边到另一个字所经过的最少边数。S_2 的任一非空子集都是一个码，故共有 2^4-1 个码。

又如长度为3的字集 $S_3=\{000, 001, 010, 011, 100, 101, 110, 111\}$ 有 2^3 个不同的字，它们可用一个立方体表示出来，如图 9–1.2(*b*)所示。每个字占据立方体的一个顶点，两个字之间如果

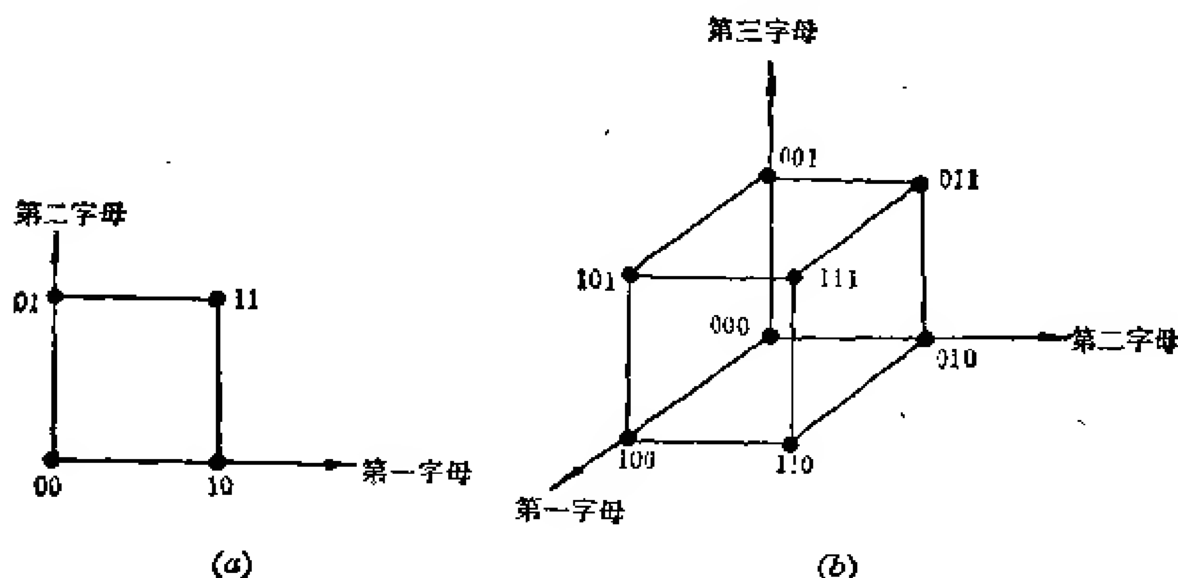


图 9–1.2

只有一个字母不同，它们就在一条棱的两端。两个字如果有两个字母不同，它们就在正方形的一条对角线的两端，如果三位都不同，它们就在正方体的对角线的两端，反之亦然。同样，两个字中不同字母的个数恰等于从一个字出发沿着立方体棱到另一个字所经过的最少棱数。V_3 的任一非空子集都是一个码，共有 2^8-1 个码。

一般，字长为 n 的不同字共有 2^n 个，它们分别是 n 立方的顶点。两个字中不同字母的个数恰等于从一个字出发沿着 n 立方棱到另一个字所经过的最少棱数。

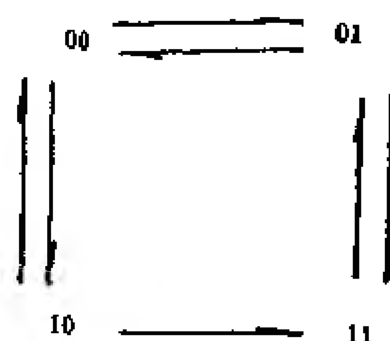


图 9-1.3

例1　考察 2 立方中的一个编码 $C_1=\{00, 01, 10, 11\}$，如果在信息传送过程中，由于噪声的干扰，可能产生一位信息错误，那么，码字 00 在第一位出错就变成 10，在第二位出错就变为 01，它们仍是码字。一般地，码 C_1 中任一码字一位出错后仍是码字。它们的关系如图 9-1.3 所示。由于一个码字出现单错后仍是码字，因此这种编码根本无法查错。

例2　考察 2 立方中的另一个编码 $C_2=\{00, 11\}$，码字 00 在第一位出错或码字 11 在第二位出错都变为 10，码字 00 在第二位出错或码字 11 在第一位出错都变为 01，而 01，10 是废码。所以，当接收到 01 或 10 时，就可知道传输中发生了单错，但不能判别是 00 出错还是 11 出错，因此，对于这种编码，虽然我们可以检查出单错，但不能纠错。

例3　考察 3 立方中的一个编码 $C_3=\{001, 110\}$，码字 001 出现单错后将变为 000，011，101。而 110 出现单错后将变为 111，100，010。由于这两个码字出现单错后，废码是不同的，因此，从接收到的字就可以确定发送字。例如，接收到 010，就可决定发送字是 110。对于这种编码，我们不仅可以检查出单错，还可以纠单错。

现在来考察信息传送的出错概率。

设 p 表示一个字母在信道中正确传送的概率，那么，由于噪声干扰，产生错误传送的概率是 $q=1-p$。假设各位字母的传送是相互独立的。那么，一个 n 位的码字中出现 r 个错误的概率是 $C_n^r p^{n-r} q^r$。其中

$$C_n^r=\frac{n!}{(n-r)!r!}$$

是从 n 位中任取 r 位的不同组合数。

9-1 习题

(1) 构造出所有长度为 2 的二进制编码。找出能检查出单错的编码。是否存在能纠正单错的编码，为什么？

(2) 写出下列单词的五单位电传码和 3:4 码：

$$CHINA,\ SHANGHAI。$$

(3) 已知字母 0,1 正确传送的概率是 0.98，试求

a) $CHINA$ 的五单位电传码只在前三位出错的概率；

b) $CHINA$ 的五单位电传码中有一位出错的概率。

(4) 一个字长十位的码字在传送过程中要求两位出错的概率不超过 10^{-3}，试求字母正确传送的概率。

9-2 线性分组码的纠错能力

在讨论线性码的纠错能力之前，先来看一个例子。

例 1 对于长度为 2 的二进制编码 $C_1=\{00, 01, 10, 11\}$，在上节已讨论过，它不能发现单错。将每一码字增加一位，使每一码字中所含 1 的个数为偶数，它们分别变成 000, 011, 101, 110，如果在传送过程中有码字发现单错，那么，它就变成含有奇数个 1 的废码。如 011 发生单错，就变成 111, 001 或 010。同样，如果在传送过程中一个码字出现三个错，那么，它也变成含有奇数个 1 的废码。因此，对于这种码，我们很易发现奇数个错误。但由于 011 在第二位出错，000 在第三位出错，101 在第一位出错都变成 001，所以不能纠正单错。

类似地，若每一码字增加一位，使每一码字中所含1的个数为奇数，它们分别变成001, 010, 100, 111，则也能发现奇数个错误，但不能纠正。

象这种增加奇偶校验位的码称为奇偶校验码，增加的位称为校验位，校验位是信息位的模2和，且每一码字都是等长的，这种码称为线性分组码。

为了进一步讨论编码的查错和纠错能力，下面再引进一些基本概念。

定义 9-2.1 设 S_n 是长度为 n 的二进制串组成的集合，$S_n=\{x_1x_2x_3\cdots x_n \mid x_i\in\{0, 1\}, 1\leqslant i\leqslant n\}$。定义 S_n 上的一个二元运算 $\oplus$，使得对任意 $X, Y\in S_n$，$X=x_1x_2\cdots x_n$，$Y=y_1y_2\cdots y_n$。

$X\oplus Y=z_1z_2\cdots z_n$，其中 $z_i=x_i+y_i$，集合 $\{0, 1\}$ 上运算 $+$ 是按位加，如表 9-2.1 所示。

表 9-2.1

+	0	1
0	0	1
1	1	0

定理 9-2.1 代数系统 $\langle S_n, \oplus\rangle$ 是群。

证明 由于 $\{0, 1\}$ 上二元运算 $+$ 是封闭和可结合的，所以，S_n 上二元运算 $\oplus$ 是封闭和可结合的。

$\overbrace{00\cdots0}^{n}$ 是幺元。S_n 中任一元素的逆元是自身。因此 $\langle S_n, \oplus\rangle$ 是群。 □

定义 9-2.2 S_n 的任一子集 C，如果 $\langle C, \oplus\rangle$ 是群，称码 C 是群码。

定义 9-2.3 对于 S_n 中任两元素 $X=x_1x_2\cdots x_n$，$Y=y_1y_2\cdots y_n$，X 和 Y 中对应位字母不同的个数，称为 X 和 Y 的海明(Hamming)距，记作 $H(X, Y)$，即

$$H(X, Y)=\sum_{i=1}^{n}(x_i+y_i)$$

例 2 设 $n=3$, 码 $\{000, 111\}$ 对运算 $\oplus$ 构成群, 它是群码, 000 与 111 三个字母都不同, 它们的海明距是 3。

例 3 设 $n=4$, $X=1001$, $Y=0100$, $Z=1000$。集合 $\{X, Y, Z\}$ 对运算 $\oplus$ 不构成群, 因为在此集合中无幺元。$H(X, Y)=3$, $H(Y, Z)=2$, $H(Z, X)=1$。

定理 9-2.2 设 $X, Y, Z\in S_n$, 那么

a) $H(X, X)=0$

b) $H(X, Y)=H(Y, X)$

c) $H(X, Y)+H(Y, Z)\geqslant H(X, Z)$

证明 令 $X=x_1x_2\cdots x_n$, $Y=y_1, y_2\cdots y_n$, $Z=z_1z_2\cdots z_n$

a) 因为 $x_i+x_i=0$, 所以

$$H(X, X)=\sum_{i=1}^{n}(x_i+x_i)=0$$

b) 因为 $x_i+y_i=y_i+x_i$, 所以

$$H(X, Y)=\sum_{i=1}^{n}(x_i+y_i)=\sum_{i=1}^{n}(y_i+x_i)=H(Y, X)$$

c) 因为 $(x_i+y_i)+(y_i+z_i)\geqslant x_i+z_i$[注], 所以

$$\begin{aligned}H(X, Y)+H(Y, Z)&=\sum_{i=1}^{n}(x_i+y_i)+\sum_{i=1}^{n}(y_i+z_i)\\&=\sum_{i=1}^{n}((x_i+y_i)+(y_i+z_i))\\&\geqslant\sum_{i=1}^{n}(x_i+z_i)=H(X, Z)\end{aligned}$$ □

定义 9-2.4 一个码 C 中所有不同码字的海明距的极小值称为码 C 的极小距, 记作 $d_{\min}(C)$。

$$d_{\min}(C)=\min_{\substack{X,Y\in C\\X\neq Y}}H(X, Y)$$

例 2 中的码的极小距是 3, 例 3 中的码的极小距是 1。

下面两条定理, 分别说明一个码的查错和纠错的能力。

定理 9-2.3 一个码 C 能查出不超过 k 个错误的充要条件是

[注] 不等式左边两个括弧式中间的"+"是普通加号, 每个括弧式内的"+"是按位加。

此码的极小距至少是 $k+1$。

证明　充分性

设码 C 的极小距 $d_{\min}(C) \geqslant k+1$，$X \in C$ 是任一码字，经过传送后，接收字为 X'，如果传送过程中，产生了错误且错误的位数 $\leqslant k$，那么 $0 < H(X, X') =$ 错误的位数 $\leqslant k$，$X' \neq X$。又 C 中任一不同于 X 的码字 Y，有 $H(X, Y) \geqslant d_{\min}(C) \geqslant k+1 > H(X, X')$，所以，$X'$ 不能是码 C 中不同于 X 的码字，即 $X' \notin C$，X' 是废码。因此，能查出不超过 k 个错误。

必要性

设码 C 能查出不超过 k 个错误，这表示与一个码字的海明距不超过 k（且 >0）的所有字都是废码，故码 C 中任两个码字的海明距至少是 $k+1$，即

$$d_{\min}(C) \geqslant k+1。\qquad \square$$

由上述定理可知例 2 中的码，极小距是 3，所以能查出单错和两个错。例 3 中的码，极小距是 1，所以不能查出单错。如码字 1001 在第四位出错，就成为另一码字 1000，不是废码。

接着讨论纠错，为此先建立一条译码准则：

最小距离译码准则：给定码 C，设接收字为 X'，在 C 中找一个码字 X，使 X' 与 X 的海明距是 X' 与 C 中所有码字海明距的极小值，即

$$H(X, X') = \min_{Y \in C} H(Y, X')$$

则我们将 X' 译为码字 X。

定理 9-2.4　一个码能纠 k 个错的充要条件是此码的极小距至少是 $2k+1$。

证明　充分性

设 $d_{\min}(C) \geqslant 2k+1$。发送字是 X，接收字是 X'，且 $H(X, X') = k$。对 C 中任一码字 $Y \neq X$，因为

$$H(X, Y) \geqslant d_{\min}(C) \geqslant 2k+1$$

所以 $H(X', Y) \geqslant H(X, Y) - H(X, X') \geqslant (2k+1) - k = k+1$，根据最小距离译码准则，$X'$ 只能译成 X，不能译成其它码字，所

以能纠正 k 个错。

必要性

设码 C 能纠正 k 个错。用反证法。如果 $d_{\min}(C)\leqslant 2k$, 那么,存在码字 $X, Y\in C$, $H(X, Y)\leqslant 2k$。由定理 9-2.3 可知, $H(X, Y)\geqslant k+1$, X 与 Y 中至少有 $k+1$ 位不同, 设发送字 X 经传送后,得接收字 X', 而 X' 与 X 中有 k 位不同, 且这 k 位恰是 X 与 Y 不同位的一部分。又因为 $H(X, Y)\leqslant 2k$, 故 X' 与 Y 的不同位数 $\leqslant k$, 即 $H(X', Y)\leqslant k$。根据最小距离译码准则, 如果 $H(X', Y)<k$, 则 X' 将被误译为 Y。如果 $H(X', Y)=k$, 则 X' 既可译为 X, 又可译为 Y。因此, 不能纠正 k 个错, 与假设矛盾。 □

根据这条定理可以知道,例 2 中的码可以纠正单错。

例 3 给定码 $C=\{000000, 001101, 010011, 011110, 100110, 101011, 110101, 111000\}$, 那么 $d_{\min}(C)=3$, 可以纠单错。如接收字是 110001, 应译为 110101。设接收字 001001 是由发送字 000000 在第三和第六位出错而得到, 但按照最小距离译码准则将误译为 001101, 因此码 C 不能纠两个错。

定理 9-2.3 和定理 9-2.4 有个简单的几何解释。以任一码字 X 为球心, 以 k 为半径, 作 n 维空间中的球。当 $d_{\min}(C)\geqslant k+1$ 时, 说明 C 中所有其它码字都落在这种球的外面, 如图 9-2.1(a)

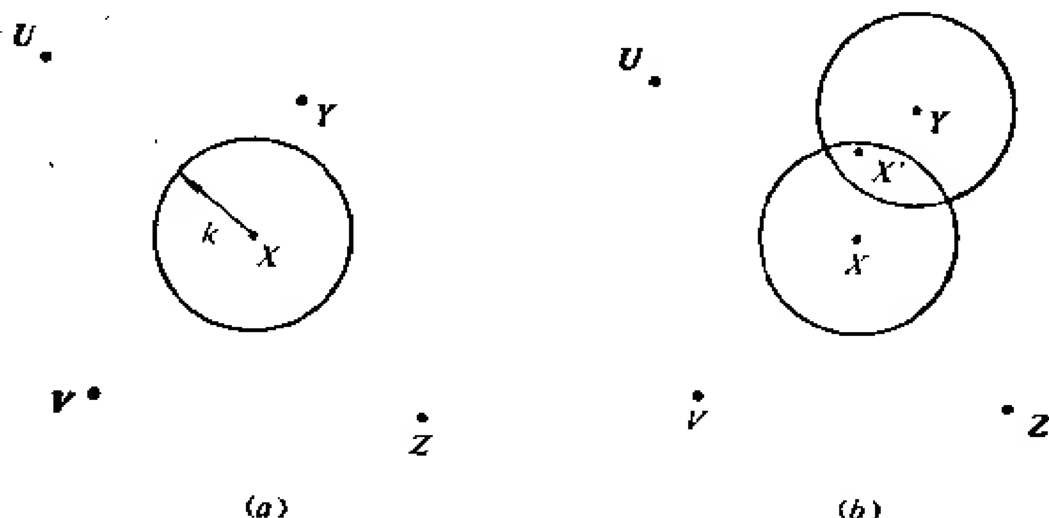


图 9-2.1

所示。设码字 X 在传送过程中，产生的错误不超过 k 个，它的接收字 X' 必在此球内，所以，我们可以查出 k 个或少于 k 个错。此外，若接收字 X' 落在分别以 X 和 Y 为球心，k 为半径的两个球的公共部分，如图 9-2.1(b) 所示。若 $H(X', Y)<H(X', X)$，根据最小距离译码准则，X' 将误译为 Y，因此，在这种情况下，码 C 不能纠 k 个错。

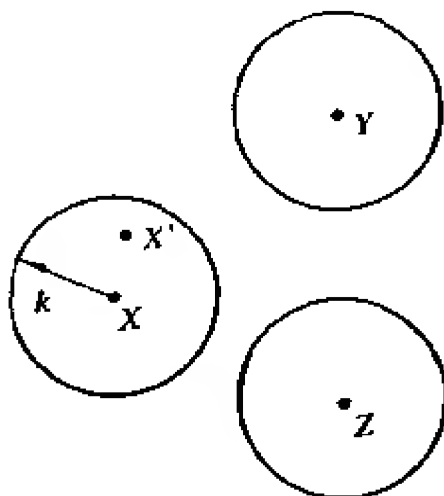


图 9-2.2

如果 $d_{\min}(C)\geqslant 2k+1$，那么，以任意码字为球心，半径为 k 的球都不相交，如图 9-2.2 所示，此时，如有传送错误 $\leqslant k$ 的接收字，它只能落在一个球内，根据最小距离译码准则，此接收字只能译为此球的球心码字，即它能纠 k 个错。

9-2 习题

(1) 给定码 $C=\{00000, 10001, 01100, 10101\}$，试求码 C 中任两个码字的海明距和 $d_{\min}(C)$。

(2) 设 X, Y, Z 是线性码 C 中三个不同的码字，写出 $H(X, Y)+H(Y, Z)=H(X, Z)$ 的充要条件，并加以证明。

(3) 证明字长不超过 $2k$ 的码不能纠 k 个错。字长不超过 k 的码不能查 k 个错。

(4) 给定线性码 C，如果 $d_{\min}(C)\geqslant k+k'+1(k'\geqslant k)$，则码 C 能查 k' 个错且能纠 k 个错。请构造一个能纠单错且能查出两个错的线性码。

9-3 海明码

海明在 1950 年提出了一种能纠单错的线性分组码，称为海明码，这种编码很简单、直观、易于实现，目前在计算机系统中经常使用。在讨论如何构造海明码之前，先看一个例子。

例 1　对于 S_4 中每一字 $a_1a_2a_3a_4$，若增加三位校验位 a_5，a_6，a_7，使其成为字长为 7 的码字 $a_1a_2a_3a_4a_5a_6a_7$，其中校验位 a_5，a_6，a_7 满足下列方程组

$$a_1+a_2+a_3+a_5=0 \tag{1}$$

$$a_1+a_2+a_4+a_6=0 \tag{2}$$

$$a_1+a_3+a_4+a_7=0 \tag{3}$$

它等价于下列方程组

$$a_5=a_1+a_2+a_3$$

$$a_6=a_1+a_2+a_4$$

$$a_7=a_1+a_3+a_4$$

故当 a_1，a_2，a_3，a_4 给定后，就可唯一确定校验位 a_5，a_6，a_7。这样，就构成了一个字长为 7 的码 C，如表 9-3.1 所示。

表　9-3.1

a_1	a_2	a_3	a_4	a_5	a_6	a_7
0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	0	1
0	0	1	1	1	1	0
0	1	0	0	1	1	0
0	1	0	1	1	0	1
0	1	1	0	0	1	1
0	1	1	1	0	0	0
1	0	0	0	1	1	1
1	0	0	1	1	0	0
1	0	1	0	0	1	0
1	0	1	1	0	0	1
1	1	0	0	0	0	1
1	1	0	1	0	1	0
1	1	1	0	1	0	0
1	1	1	1	1	1	1

考察方程(1)到(3)。显然，对于 C 中任一码字，如果在传送过程中，发生了单错，那么，这些方程中必有一个或几个不满足。为

了根据出错的方程决定码字的出错位。先建立三个谓词：

$$P_1(a_1,\ a_2,\ \cdots,\ a_7):\quad a_1+a_2+a_3+a_5=0$$

$$P_2(a_1,\ a_2,\ \cdots,\ a_7):\quad a_1+a_2+a_4+a_6=0$$

$$P_3(a_1,\ a_2,\ \cdots,\ a_7):\quad a_1+a_3+a_4+a_7=0$$

对任一字 $a_1a_2a_3a_4a_5a_6a_7$，当右端方程满足时，则 P_i 为真，否则为假。例如对于字 0001101，$P_1(0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1)$为假，$P_2(0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1)$为假，$P_3(0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1)$为真。

令 S_i 是 P_i 中所出现的变元组成的集合，即 $S_1=\{a_1,\ a_2,\ a_3,\ a_5\}$，$S_2=\{a_1,\ a_2,\ a_4,\ a_6\}$，$S_3=\{a_1,\ a_3,\ a_4,\ a_7\}$。因为 S_i 中任一元素是字 $a_1a_2a_3a_4a_5a_6a_7$ 中的一个字母，显然 S_i 就是使 P_i 为假的所有可能出错字母的集合。上述三个集合可组成七个互不相交的非空集合如下：

$$S_1\cap S_2\cap S_3=\{a_1\},\qquad S_1\cap S_2\cap \sim S_3=\{a_2\}$$

$$S_1\cap \sim S_2\cap S_3=\{a_3\},\qquad S_1\cap \sim S_2\cap \sim S_3=\{a_5\}$$

$$\sim S_1\cap S_2\cap S_3=\{a_4\},\qquad \sim S_1\cap S_2\cap \sim S_3=\{a_6\}$$

$$\sim S_1\cap \sim S_2\cap S_3=\{a_7\}$$

从这七个集合，我们可决定出错位。例如 $\sim S_1\cap S_2\cap S_3=\{a_4\}$，即 $a_4\notin S_1$，$a_4\in S_2$，$a_4\in S_3$，所以，如果 a_4 位出错，则 P_1 为真，而 P_2，P_3 为假，反之亦然，以此类推，我们就可得到译码表如表 9-3.2 所示。

表 9-3.2

P_1	P_2	P_3	出错字母
T	T	T	无
T	T	F	a_7
T	F	T	a_6
T	F	F	a_4
F	T	T	a_5
F	T	F	a_3
F	F	T	a_2
F	F	F	a_1

例如，接收字是1000011，代入方程(1)，(2)和(3)，可知方程(1)不满足，方程(2)和(3)满足，P_1 为 $\boldsymbol{F}$，P_2 和 P_3 为 $\boldsymbol{T}$，由表9-3.2可知出错字母是 a_5，因此，发送字是1000111。又如接收字是0111111，代入方程(1)，(2)和(3)，可知这些方程都不满足，P_1，P_2，P_3 都为 $\boldsymbol{F}$，由表9-2.3可知出错字母是 a_1，因此发送字是1111111。

例1所构造的单错可纠码，它由方程(1)，(2)和(3)决定。这三个方程的矩阵形式为

$$\vec{X}\cdot H^T=\mathbf{0}$$

其中，$\vec{X}=(a_1,\ a_2,\ \cdots,\ a_7)$，它是码字 $X=a_1a_2\cdots a_7$ 所对应的向量。

$$H=\begin{pmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}$$

H^T 是 H 的转置矩阵。

因此，一个线性分组码就由矩阵 H 确定，而它的纠错能力可由 H 的特性来决定。下面就来讨论矩阵 H 的构造。

定义 9-3.1 一个码字 X 中所含1的个数，称为此码字的重量，记作 $W(X)$。

例如码字11010和01100的重量分别为3和2。又如码字 $000\cdots0$ 的重量是0，为了方便起见，将码字 $000\cdots0$ 记作 $\mathbf{0}$。

定理 9-3.1 给定码 C，对于任两个码字 $X,Y\in C$，有

$$H(X,Y)=H(X\oplus Y,\mathbf{0})=W(X\oplus Y)$$

证明 设 $X=x_1x_2\cdots x_n$，$Y=y_1y_2\cdots y_n$，$Z=X\oplus Y=z_1z_2\cdots z_n$，$z_i=x_i+y_i\ (1\leqslant i\leqslant n)$，$H(X,Y)=\sum\limits_{i=1}^{n}(x_i+y_i)=\sum\limits_{i=1}^{n}z_i=\sum\limits_{i=1}^{n}(z_i+0)=H(X\oplus Y,\mathbf{0})$，因为 $\sum\limits_{i=1}^{n}z_i=W(Z)$，所以 $H(X,Y)=H(X\oplus Y,\mathbf{0})=W(X\oplus Y)$。 □

定理 9-3.2 群码 C 中非零码字的最小重量等于此群码的最小距。即

$$\min_{\substack{Z\in C\\ Z\neq 0}} W(Z)=d_{\min}(C)$$

证明　因为 $\langle C, \oplus\rangle$ 是群，幺元 $\mathbf{0}\in C$。

对于任一非零码字 Z，

$$W(Z)=W(Z\oplus\mathbf{0})=H(Z, \mathbf{0})$$

$$\geqslant \min_{\substack{X,Y\in C\\ X\neq Y}} H(X, Y)=d_{\min}(C)$$

所以

$$\min_{\substack{Z\in C\\ Z\neq 0}} W(Z)\geqslant d_{\min}(C)$$

此外，对于 C 中任两个不同码字 X, Y，由于 $\oplus$ 封闭性，$X\oplus Y\in C$，且 $X\oplus Y\neq\mathbf{0}$，有

$$H(X, Y)=W(X\oplus Y)\geqslant\min_{\substack{Z\in C\\ Z\neq 0}} W(Z)$$

所以

$$d_{\min}(C)=\min_{\substack{X,Y\in C\\ X\neq Y}} H(X, Y)\geqslant\min_{\substack{Z\in C\\ Z\neq 0}} W(Z)$$

因此

$$\min_{\substack{Z\in C\\ Z\neq 0}} W(Z)=d_{\min}(C)$$ □

例 2　a) $C_1=\{0000, 1111\}$ 是群码，

$$\min_{\substack{Z\in C_1\\ Z\neq 0}} W(Z)=W(1111)=4=H(0000, 1111)$$

$$=d_{\min}(C)$$

b) $C_2=\{001, 010, 100\}$ 不是群码，而

$$\min_{\substack{Z\in C_2\\ Z\neq 0}} W(Z)=1,\ d_{\min}(C_2)=2$$

所以

$$\min_{\substack{Z\in C_2\\ Z\neq 0}} W(Z)<d_{\min}(C_2)$$

c) $C_3=\{110, 111\}$ 不是群码，而

$$\min_{\substack{Z\in C_3\\ Z\neq 0}} W(Z)=2,\ d_{\min}(C_3)=1$$

所以

$$\min_{\substack{Z\in C_3\\ Z\neq 0}} W(Z)>d_{\min}(C_3)$$

定理 9-3.3　设 H 是 k 行 n 列矩阵，$X=x_1x_2\cdots x_n$ 是 n 位二进制串，那么集合

$$G=\{X \mid \vec{X}\cdot H^T=\mathbf{0}\}$$

对于运算 $\oplus$ 构成群，即 G 是群码。

证明　因为 $\langle S_n, \oplus\rangle$ 是有限群，设 $X, Y\in G$，那么，$\vec{X}\cdot H^T=\mathbf{0}$，$\vec{Y}\cdot H^T=\mathbf{0}$，$(\overrightarrow{X\oplus Y})\cdot H^T=(\vec{X}\cdot H^T)\oplus(\vec{Y}\cdot H^T)=\mathbf{0}\oplus\mathbf{0}=\mathbf{0}$

所以，$X\oplus Y\in G$，由定理 5-4.7 可知 $\langle G, \oplus\rangle$ 是子群，即 G 是群码。 □

由本定理可知例 1 的码是群码。

定义 9-8.2　群码 $G=\{X \mid \vec{X}\cdot H^T=\mathbf{0}\}$ 称为由 H 生成的群码，G 中每一码字，称为由 H 生成的码字，矩阵 H 称为一致校验矩阵。

矩阵 H 的 n 个列向量分别记为 h_1，h_2，…，h_n，其中 h_i 是第 i 个列向量，即

$$H=(h_1h_2\cdots h_n)$$

其中

$$h_i=\begin{pmatrix} h_{1i}\\ h_{2i}\\ \vdots\\ h_{ki}\end{pmatrix}$$

定义列向量 h_i 与 h_j 的和 $h_i\oplus h_j$ 为

$$h_i\oplus h_j=\begin{pmatrix} h_{1i}+h_{1j}\\ h_{2i}+h_{2j}\\ \vdots\\ h_{ki}+h_{kj}\end{pmatrix}$$

定理 9-8.4　一致校验矩阵 H 生成一个重量为 q 的码字的充要条件是在 H 中存在 q 个列向量，它们的和为 $\mathbf{0}$。

证明　充分性

如果在 H 中有 q 个列向量 h_{i_1}，h_{i_2}，…，h_{i_q}，满足

$$h_{i_1}\oplus h_{i_2}\oplus\cdots\oplus h_{i_q}=\mathbf{0}$$

构造一个字 $X=x_1x_2\cdots x_n$，其中 $x_{i_1}=x_{i_2}=\cdots=x_{i_q}=1$，其它为 0，显然，对此字 X，

$$\vec{X}\cdot H^T=(h_{i_1}\oplus h_{i_2}\oplus\cdots\oplus h_{i_q})^T=\mathbf{0}$$

所以，X 是由 H 生成的重量为 q 的码字。

必要性

如果 H 生成重量为 q 的码字 X，$X=x_1x_2\cdots x_n$，其中 $x_{i_1}=x_{i_2}=\cdots=x_{i_q}=1$，其余为 0，那么，由 $X\cdot H^T=\mathbf{0}$ 得到

$$h_{i_1}\oplus h_{i_2}\oplus h_{i_3}\oplus\cdots\oplus h_{i_q}=\mathbf{0}$$

因此，q 个列向量 h_{i_1}，h_{i_2}，$\cdots$，h_{i_q}，它们的和为 $\mathbf{0}$。 □

推论：由 H 生成的群码中非零码字的最小重量等于矩阵 H 中列向量和为 $\mathbf{0}$ 的最小向量数。

如果矩阵 H 中列向量和为 $\mathbf{0}$ 的最小向量数是 1，则在 H 中恰存在一个列向量为零向量。

如果矩阵 H 中列向量和为 $\mathbf{0}$ 的最小向量数是 2，则在 H 中恰存在两个相同的列向量。

例 1 中矩阵 H 没有零向量且各个列向量互不相同，但它的第二、三、四列向量之和为 $\mathbf{0}$，所以，列向量和为 $\mathbf{0}$ 的最小向量数是 3，由推论可知，此 H 生成的群码的非零码字最小重量是 3，因此，由定理 9-3.2 可知，此群码的最小距是 3，再由定理 9-2.4 可知，此群码必可纠单错。

此外，线性分组码 C 中每一码字 X 形式为：

$$X=\underbrace{x_1x_2\cdots x_m}_{\text{信息位}}\underbrace{x_{m+1}\cdots x_{m+k}}_{\text{校验位}}$$

k 位校验位与 m 位信息位之间有如下关系：

$$x_{m+i}=q_{i1}x_1+q_{i2}x_2+\cdots+q_{im}x_m \quad (1\leqslant i\leqslant k)$$

其中 $q_{ij}\in\{0, 1\}$，$1\leqslant j\leqslant m$。

令 $$H=\left(\boxed{Q}_{k\times m}\quad \boxed{I_k}_{k\times k}\right)$$

其中 $$Q=\begin{pmatrix} q_{11} & \cdots & q_{1m} \\ \vdots & & \vdots \\ q_{k1} & \cdots & q_{km} \end{pmatrix}_{k\times m},\quad I_k=\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{k\times k}$$

那么，码 C 中任一码字满足方程

$$X\cdot H^T=\mathbf{0}$$

记 $n=m+k$, 这种码简称为 (n, m) 码。

为了要使码 C 能纠正单错，由定理9-2.4, 9-3.3及定理9-3.4的推论可知，要求 H 中的列向量均不相同且无零向量，即矩阵 Q 的列向量不能为 $\mathbf{0}$ 且不能出现 I_k 中的 k 个列向量。因为 Q 的每一列向量都是 k 维的，可有 2^k 个不同的列向量，因此，可从 2^k-1-k 个列向量中任取 m 个来组成 Q。

故必须满足 $m\leqslant 2^k-1-k$ 或 $2^k\geqslant(m+k)+1=n+1$。

例 3 $n=7$, 则 $2^k\geqslant 7+1=8$, $k\geqslant 3$, 如取 $k=3$, 则 $m=n-k=4$, 即每一码字中四位是信息位，三位是校验位，且一致校验矩阵为

$$H=\begin{pmatrix} & 1 & 0 & 0\\ Q_{3\times 4} & 0 & 1 & 0\\ & 0 & 0 & 1\end{pmatrix}$$

其中矩阵 Q 有四个列向量，而 $2^k-1-k=2^3-1-3=4$, 因此 Q 的四个列向量是唯一决定的，它们只能是

$$\begin{pmatrix}1\\1\\1\end{pmatrix},\ \begin{pmatrix}1\\1\\0\end{pmatrix},\ \begin{pmatrix}1\\0\\1\end{pmatrix},\ \begin{pmatrix}0\\1\\1\end{pmatrix}$$

如果选取

$$Q=\begin{pmatrix}1 & 1 & 1 & 0\\ 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1\end{pmatrix}$$

此时
$$H=\begin{pmatrix}1 & 1 & 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 1 & 0 & 0 & 1\end{pmatrix}$$

就是例1中的矩阵。

此外，若将上述矩阵 Q 中列向量作交换，则也不能构成新的码，因此，例1中的(7, 4)码是唯一的。

如取 $k=4$, 则 $m=n-k=3$

$$H=\begin{pmatrix} & 1 & 0 & 0 & 0 \\ Q_{4\times 3} & 0 & 1 & 0 & 0 \\ & 0 & 0 & 1 & 0 \\ & 0 & 0 & 0 & 1 \end{pmatrix}$$

矩阵 Q 有三个列向量，而 $2^4-1-4=11$，可有 $C_{11}^3=165$ 种组成 Q 的方法，即可有 165 个不同的(7, 3)码。

例如，下面都是一致校验矩阵：

$$H_1=\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$H_2=\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$H_3=\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

矩阵 H_1 中第一列，第四列，第五列三个列向量之和为零向量，所以，它对应的码只能纠单错。同样，矩阵 H_2, H_3 对应的码也只能纠单错。

例 4　$n=9$, $2^k\geqslant 9+1=10$, $k\geqslant 4$。如取 $k=4$，则 $m=9-4=5$。一致校验矩阵 H 中 Q 有 5 个列向量，而 $2^k-1-k=2^4-1-4=11$，构成 Q 就可有 $C_{11}^5=462$ 种组成 Q 的方法，即可有 462 个不同的(9, 5)码。

9-3　习题

(1) 构造一个可纠单错的(9, 5)码。

(2) 设 C 是一个线性分组码，它同时具有偶数重量和奇数重量的码字。

证明：偶数重量码字的数目等于奇数重量码字的数目。

(3) 考察一个(8, 4)码 C，它的校验位 a_5, a_6, a_7, a_8 满足下列方程

$$a_5 = a_1 + a_2 + a_4$$

$$a_6 = a_1 + a_3 + a_4$$

$$a_7 = a_1 + a_2 + a_3$$

$$a_8 = a_2 + a_3 + a_4$$

其中 a_1, a_2, a_3, a_4 为信息位。

求出这个码的一致校验矩阵。证明 $\min\limits_{\substack{X \in C \\ X \neq 0}} W(X) = 4$。

(4) 写出例 3 中一致校验矩阵 H_1 的(7, 3)码中所有码字，并求出此码中非零码字的最小重量。

(5) 求出海明码中校验位数不超过信息位数的最小信息位数。

9-4 查表译码法

在上节例 1 中给出了纠单错的方法，但这个方法比较繁琐，现介绍查表译码法。

给定海明码 C，它的每一码字，信息位长度为 m，校验位长度为 $k = n - m$，$\langle C, \oplus \rangle$ 是 $\langle S_n, \oplus \rangle$ 的子群。

设发送字是 X，且传送过程中在第 i 位发生错误，接收字是 X'。令 $e_i = \overbrace{0 \cdots 010 \cdots 0}^{n}$，其中 1 恰在第 i 位，显然，$X' = X \oplus e_i$，$X = X' \oplus e_i$，$H(X, X') = W(X \oplus X') = W(e_i) = 1$，根据最小距离译码准则接收字 X' 应被译为 X。

因为海明码 C 可纠单错，$\min\limits_{\substack{X \in C \\ X \neq 0}} W(X) \geqslant 3$，即 C 中除零码字 $(\overbrace{00 \cdots 0}^{n})$ 外，不包含重量不超过 2 的字，所以 $e_i \notin C (1 \leqslant i \leqslant n)$。在群 $\langle S_n, \oplus \rangle$ 中，确定 C 关于 e_i 的左陪集 $e_i \oplus C$，这种左陪集共有 n 个。

由拉格朗日定理可知，C 在 S_n 中的左陪集应有 $|S_n| / |C| = 2^{n-m} = 2^k$ 个。因为 $2^k \geqslant n + 1$。

当 $2^k = n + 1$ 时，

$$\bigcup_{i=1}^{n}(e_i \oplus C) \cup C = S_n$$

当 $2^k > n+1$ 时，

$$\bigcup_{i=1}^{n}(e_i \oplus C) \cup C \subset S_n$$

所以还须继续构造陪集。

具体构造可以这样进行：

1．将 C 中所有码字组成第一行，零码字作为首项。

2．构造所有陪集 $e_1 \oplus C$, $e_2 \oplus C$, …, $e_n \oplus C$ 分别组成第二行，第三行，…，第 $n+1$ 行，使得陪集 $e_i \oplus C$ 中元素 $e_i \oplus c_j (c_j \in C)$，与元素 c_j 在同一列。

3．如果 $2^k = n+1$，过程结束。如果 $2^k > n+1$，则取一个不在 C 且不在已有陪集中的字 z，构造陪集 $z \oplus C$，使元素 $z \oplus c_j$ 与元素 c_j 在同一列，以此类推，直至 2^k 个陪集构造完毕。如表 9-4.1 所示。其中

$$p = 2^k - (n+1)$$

表 9-4.1

C:	c_1（零码字）	c_2	c_3	…	c_{2^m}
$e_1 \oplus C$:	$e_1 \oplus c_1$	$e_1 \oplus c_2$	$e_1 \oplus c_3$	…	$e_1 \oplus c_{2^m}$
$e_2 \oplus C$:	$e_2 \oplus c_1$	$e_2 \oplus c_2$	$e_2 \oplus c_3$	…	$e_2 \oplus c_{2^m}$
	…	…	…		
$e_n \oplus C$:	$e_n \oplus c_1$	$e_n \oplus c_2$	$e_n \oplus c_3$	…	$e_n \oplus c_{2^m}$
$z_1 \oplus C$:	$z_1 \oplus c_1$	$z_1 \oplus c_2$	$z_1 \oplus c_3$	…	$z_1 \oplus c_{2^m}$
	…	…	…		
$z_p \oplus C$:	$z_p \oplus c_1$	$z_p \oplus c_2$	$z_p \oplus c_3$	…	$z_p \oplus c_{2^m}$

利用上表，我们就可以进行译码。

设接收字为 X'，它在 i 行 j 列，那么，X' 的发送字为 c_j，且 i 行首项元素中字母 1 的所在位就是传送过程中的出错位，这种译码方法称为查表译码法。

例 1　设 $m=3$, $n=6$，一致校验矩阵是

$$H=\begin{pmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\1&1&1&0&0&1\end{pmatrix}$$

则它的校验位满足下列方程

$$a_4=a_1+a_2$$
$$a_5=a_1+a_3$$
$$a_6=a_1+a_2+a_3$$

因为 H 中的列向量都不相同且无零向量，$h_1 \oplus h_2 \oplus h_5 = \mathbf{0}$，所以，$H$ 对应的线性分组码 C 可以纠单错。

$C=\{000000, 001011, 010101, 011110, 100111,$
$101100, 110010, 111001\}$

它的译码表如表 9-4.2 所示。

表 9-4.2

000000	001011	010101	011110	100111	101100	110010	111001
100000	101011	110101	111110	000111	001100	010010	011001
010000	011011	000101	001110	110111	111100	100010	101001
001000	000011	011101	010110	101111	100100	111010	110001
000100	001111	010001	011010	100011	101000	110110	111101
000010	001001	010111	011100	100101	101110	110000	111011
000001	001010	010100	011111	100110	101101	110011	111000
000110	001101	010011	011000	100001	101010	110100	111111

如果以表 9-4.2 中打方框的字为接收字，则它们对应的发送字和出错位可用表 9-4.3 所示。

表 9-4.3

接收字	接收字所在行，列	发送字	出错位
000110	[8, 1]	000000	4, 5
000011	[4, 2]	001011	3
100110	[7, 5]	100111	6
110010	[1, 7]	110010	无
101001	[3, 8]	111001	2

综上所述，当译码表为表 9-4.2 时，码 C 不仅能纠单错且在第四、五位同时出错时也能纠正。

9-4 习题

(1) 给定字长 n 位的海明码 C，证明 $e_j \notin C \cup (e_1 \oplus C) \cup (e_2 \oplus C) \cup \cdots \cup (e_{j-1} \oplus C)$，其中 $e_i = \overbrace{0\cdots010\cdots0}^{n}$，1 恰在第 i 位，$1 \leqslant i \leqslant n$。

(2) 给定(7, 4)码，它的一致校验矩阵是

$$H=\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

构造译码表并求接收字 1000111, 0110010 和 1111111 的发送字。

(3) 给定码 $C=\{00000, 11111\}$，证明它是一个群码。并能纠两个传送错误。构造译码表，确定接收字为 00101, 01110, 11011, 01011 和 11111 的发送字。

(4) 考察一个(8, 4)码，它的校验位 a_5, a_6, a_7, a_8 满足下列方程。

$$\begin{aligned} a_5 &= a_1 + a_2 + a_3 + a_4 \\ a_6 &= a_1 + a_2 \\ a_7 &= \quad\; a_2 + a_3 \\ a_8 &= \quad\quad\quad a_3 + a_4 \end{aligned}$$

构造译码表，并求接收字 00011010, 11110000, 10000111 的发送字。

符 号 表

数理逻辑

$\neg P$	P 的否定
$P \wedge Q$	P 与 Q 的合取
$P \vee Q$	P 与 Q 的析取
$P \rightarrow Q$	如 P 则 Q
$P \rightleftarrows Q$	P 当且仅当 Q
$P \uparrow Q$	P 与 Q 的与非
$P \downarrow Q$	P 与 Q 的或非
$P \bar{\vee} Q$	P 与 Q 的不可兼析取
$P \overset{c}{\rightarrow} Q$	P 与 Q 的条件否定
$\boldsymbol{T}$	真；重言式
$\boldsymbol{F}$	假；矛盾式
$P \Rightarrow Q$	P 蕴含 Q
$P \Leftrightarrow Q$	P 与 Q 等价
A^*	A 的对偶式
$\forall$	全称量词
$\exists$	存在量词
wff$A$	合式公式 A

集合论

$a \in A$	a 属于 A
$a \notin A$	a 不属于 A
$A \subseteq B$	A 包含于 B 中
$A \subset B$	A 真包含于 B 中
$\emptyset$	空集
E	全集
$\mathscr{P}(A)$	A 的幂集

$A\cap B$	A 与 B 的交
$A\cup B$	A 与 B 的并
$A-B$	A 与 B 的差
$\sim A$	A 的绝对补
$A\oplus B$	A 与 B 的对称差
$\lvert A\rvert$	有限集 A 的元素个数
$\lfloor x\rfloor$	小于或等于 x 的最大整数
$A\times B$	集合 A 和 B 的笛卡尔乘积
$\mathrm{dom}\,R(\mathrm{dom}f)$	关系 R 的前域(函数 f 的定义域)
$\mathrm{ran}\,R(\mathrm{ran}f)$	关系 R 的值域(函数 f 的值域)
$\mathrm{FLD}R$	关系 R 的域
I_X	集合 X 上的恒等关系
$A\sim B$	集合 A 与集合 B 等势
$B\circ S$	关系 R 和 S 的复合
A^n	n 个集合 A 的笛卡尔积
$R^{(n)}$	关系 R 的 n 次复合
R^c	关系 R 的逆关系
$r(R)$	关系 R 的自反闭包
$s(R)$	关系 R 的对称闭包
R^+、$t(R)$	关系 R 的传递闭包
R^*、$tr(R)$	关系 R 的自反传递闭包
A/R	集合 A 关于 R 的商集
C_r	最大相容类
$C_r(A)$	A 的完全复盖
$\preccurlyeq$	偏序关系
$x\equiv y(\mathrm{mod}\,m)$	$x-y$ 被 m 整除
$\mathrm{LUB}A$	A 的最小上界
$\mathrm{GLB}A$	A 的最大下界
f^{-1}	函数 f 的逆函数
$g\circ f$	函数 f 和 g 的复合

ψ_A	集合 A 的特征函数
$\psi_{\underset{\sim}{A}}$	模糊子集 $\underset{\sim}{A}$ 的隶属函数
A^+	集合 A 的后继集
$k[A]$、$\overline{\overline{A}}$	集合 A 的基
$\aleph_0$	可数集的基
$\aleph$	连续统的势

代数系统

I	整数集合
I_+	正整数集合
I_E	偶数集合
N	自然数集合
Q	有理数集合
R	实数集合
C	复数集合
N_k	集合 $\{0, 1, 2, \cdots, k-1\}$
Z_m	I 上模 m 的同余类集合
$\mathrm{GCD}(x, y)$	x, y 的最大公约数
$\mathrm{LCM}(x, y)$	x, y 的最小公倍数
$+_k$	模 k 的加法运算
$\times_k$	模 k 的乘法运算
S_n	n 个元素的集合 S 上所有置换构成的对称群
$\psi(\pi)$	在置换 π 作用下不变元的个数
$\eta(s)$	使元素 s 保持不变的置换个数
aH	H 关于 a 的左陪集
Ha	H 关于 a 的右陪集
$\mathrm{Ker}(f)$	f 的同态核
$a \prec b$	$a \preccurlyeq b$ 且 $a \neq b$
$a \vee b$	a 与 b 的最小上界
$a \wedge b$	a 与 b 的最大下界

$\bar{a}$	a 的补元素

图论

$V(G)$	图 G 的结点集合
$E(G)$	图 G 的边集合
K_n	n 个结点的完全图
$\deg(v)$	结点 v 的度数
$\Delta(G)$	$\max\{\deg v \mid v \in V(G)\}$、图 G 的最大度
$\delta(G)$	$\min\{\deg v \mid v \in V(G)\}$、图 G 的最小度
$W(G)$	图 G 的连通分支数
$k(G)$	$\min\{\|V_1\| \mid V_1$ 是 G 的点割集$\}$、G 的点连通度
$\lambda(G)$	$\min\{\|E_1\| \mid E_1$ 是 G 的边割集$\}$、G 的边连通度
$d\langle u.v\rangle$	结点 u 和 v 之间的距离
$D=\max\limits_{u,v\in V} d\langle u, v\rangle$	图的直径
$\deg(r)$	面的次数
A^n	布尔矩阵 A 的 n 次积
$A^{(n)}$	布尔矩阵 A 的 n 次布尔积
$M(G)$	无向图 G 的完全关联矩阵
	有向图 G 的完全关联矩阵
$C(G)$	图 G 的闭包
G^*	图 G 的对偶图
$x(G)$	图 G 的着色数
$C(e)$	边 e 的权
$C(T)$	树 T 的所有权之和

自动机和编码

V	字母表
λ	空串
Λ	空串组成的集合

V^*	字母表 V 上所有串的集合
V^+	字母表 V 上所有非空串的集合
$\omega\circ\varphi$	串 ω 与串 φ 连接而成的串
ω'	串 ω 的逆
Φ	空语言
L	字母表 V 上的一个语言
$L_1\circ L_2$	L_1 中任一串与 L_2 中任一串连接组成的语言
L'	语言 L 中每一个串的逆组成的语言
V_N	非终结符集
V_T	终结符集
P	生成式集
σ	开始符
$\alpha\to\beta$	生成式
$\omega\Rightarrow\hat{\omega}$	$\hat{\omega}$ 是 ω 的直接派生
$\omega\overset{*}{\Rightarrow}\hat{\omega}$	$\hat{\omega}$ 是 ω 的派生
Q	状态的有限集
S	有限输入字母表
R	有限输出字母表
q_I	初态
f: $Q\times S\to Q$	状态转换函数
g: $Q\times S\to R$	转换赋值机的输出函数
h: $Q\to R$	状态赋值机的输出函数
O: $Q\times S^+\to R$	两类自动机通用的输出函数
$M_1\sim M_2$	有限状态机 M_1 与 M_2 等价
$q_a\sim q_b$	状态 q_a 与 q_b 等价
$q_a\overset{k}{\sim}q_b$	状态 q_a 与 q_b k-等价
I	初态集
F	终态集

$\delta: Q \times S \to Q$　　转换关系

$H(X, Y)$　　X 与 Y 的海明距

$d_{\min}(C)$　　码 C 的极小距

$\vec{X}$　　码字 X 对应的向量

$W(X)$　　码字 X 的重量

参 考 文 献

[1] Abbott, J. C., "Set, Lattices, and Boolean Algebras", Allyn and Bacon, Inc., Boston, 1969.

[2] Aho, A. V., J. E. Hopcroft, and J. D. Ullman, "The Design and Analysis of Computer Algorithms", Reading, Mass.: Addison-Wesley, 1974.

[3] Bellman, Richard, Kenneth L. Cooke, and Jo Ann Lockett, "Algorithms, Graphs and Computers", New York: Academic Press, 1970.

[4] Bondy, J. A., and U. S. R. Murty, "Graph Theory with Applications", Am. Elsevior New York, 1976.

[5] Brualdi, Richard A., "Introduction to Error-Correcting Codes", Prentice-Hall, Inc., 1970.

[6] Denning, Peter J., Jack B. Dennis, Joseph E. Qualitz, "Machines, Languages, and Computation", Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1978.

[7] Deo, Narsingh, "Graph Theory with Applications to Engineering and Computer Science", Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1974.

[8] Gilbert, William J., "Mordern Algebra with Applications", John Wiley & Sons. Inc., 1976.

[9] Gill, Arthur, "Applied Algebra for the Computer Sciences", Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1976.

[10] Harary Frank, "Graph Theory", New York Addison-Wesley, 1969.

[11] Hennie, Fred, "Introduction to Computability", Addison-Wesley Publishing Company, Inc., 1977.

[12] Hopcroft, J. E., J. D. Ullman, "Introduction to Automata Theory, Languages, and Computation", Addison-Wesley Publishing Company, Inc., 1979.

[13] Kohavi, Zvi, and Azaria Paz, "Theory of Machines and Computations", Academic Press New York and London, 1971.

[14] Lin, Shu, "An Introduction to Error-Correcting Codes", Prentice-Hall, In., 1970.

[15] Liu, C. L., "Elements of Discrete Mathematics", McGraw-Hill Book Company, New York, 1968.

[16] Malitz, Jerome, "Introduction to Mathematical Logic", Springer-Verlag New York, Inc., 1979.

[17] Manna, Zohar, "Mathematical Theory of Computation", McGraw-Hill, 1974.

[18] Marcus, Marvin, "Introduction to Modern Algebra", Marcel Dekker, Inc., 1978.

[19] Preparata, Franco P., Raymond T. Yeh, "Introduction to Discrete Structures for Computer Science and Engineering", Addison-Wesley Publishing Company, 1973.

[20] Stoll, Robert R., "Set Theory and Logic", San Fransisco: W. H. Freeman and Co., 1963.

[21] Stone, Harold S., "Discrete Mathematical Structures", Chicago: Science Research Associates, 1973.

[22] Trembley, J. P., and R. Manohar, "Discrete Mathematical Structures with Applications to Computer Science", McGraw-Hill Book Company, New York, 1975.

[23] 希尔柏脱，阿克曼著："数理逻辑基础"，莫绍揆译，科学出版社。

[24] F. 豪斯道夫著："集论"，张义良、颜家驹译，科学出版社。